Confidential

Sample 御中

プラットフォーム脆弱性診断レポート

本レポートはSample 様のプラットフォームに対して脆弱性診断を行った結果をご報告するものです。レポート内には非常に重要な機密事項が含まれます。外部の悪意ある攻撃者に漏洩するとセキュリティ上、非常に大きなリスクとなります。お取り扱いには十分な注

2018年××月××日
サイバーセキュリティソリューションズ株式会社

CYBER SECURITY solutions

1．診断対象 IP アドレス

1	192.168.1.2

2．診断日時

開始日時	2018年××月××日（×）10時00分
修了日時	2018年××月××日（水）18時00分

3．診断方法

ポートスキャンおよびクレデンシャルスキャンによる

用語説明

ポートスキャンとは

攻撃者は一般的に相手ホストにダメージを与える、もしくは侵入するといったとき、事前の準備として、ポートスキャンと呼ばれる調査を行います。これは「外部から対象サーバへアクセスが可能か？」「脆弱性のあるサービスが動いていないか？」を調べる作業です。本脆弱性診断では、ポートスキャンを実施して、アクティブになっているポートを調査し、それが既知の脆弱性を持つサービスかどうか、侵入や破壊行為、クラッキング行為の恐れがないかどうかを調査します。

クレデンシャル（認証資格情報）スキャンとは

クレデンシャルスキャンはネットワークに公開されていないアプリケーションとオペレーティングシステム部分の脆弱性や、スキャナとホストの間に位置するファイアウォールに隠されている可能性のある脆弱性の発見に有効です。それにより脆弱性に関する検証を、より広い範囲で行うことが可能です。また、認証されたスキャンにより、ソフトウェアアプリケーションおよびパッケージをチェックしパッチを検証します。

※Webブラウザ　（Google Chrome）やAdobe Flash Player、Adobe（PDF）Reader、Java、Microsoft Office（Word/Excel/PowerPoint/Outlookなど）といったスタンダードなアプリケーションの脆弱性の発見に有効です。

４．共通脆弱性識別子「CVE」について

各レポート内に(CVE-2017-8675)といった記述がなされているものがあります。これは共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)と言われるもので、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子です。個別製品中の脆弱性に一意の識別番号「CVE識別番号(CVE-ID)」を付与することにより、組織Aの発行する脆弱性対策情報と、組織Xの発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したり

５．脆弱性の算定基準「CVSS」と「SEVERITY」について

脆弱性の算定基準については汎用的な評価手法の確立と普及を目指し、米国家インフラストラクチャ諮問委員会（ NIAC: National InfrastrCVSS （ Common Vulnerability Scoring System) を基に算出しています。一般的に数値が大きいほど緊急度を要し、個々の脆弱

■値の算出方法

CVSSでは、(1)脆弱性の技術的な特性を評価する基準(基本評価基準：Base Metrics)、(2)ある時点における脆弱性を取り巻く状況を評価する基準(現状評価基準：Temporal Metrics)、(3)利用者環境における問題の大きさを評価する基準(環境評価基準：Environmental Metrics)

■深刻度（SEVERITY）レベル分け

CVSS v3では、深刻度レベル分けを次のように設定しています。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

診断結果

重大度	種類数
CRITICAL	5
HIGH	51
MEDIUM	7
LOW	1

評価

評価	C

AAA	AA	A	B	C
脆弱性0個	LOWが検出された	MEDIUMが検出された	HIGHが検出された	CRITICALが検出された

総合評価

危険な状態です

プラットフォーム脆弱性診断を実施した結果、重大度「CRITICAL」「HIGH」「MEDIUM」が検出されましたので、総合評価は「Ｃ」評価となります。企業として安全な情報セキュリティ環境の目安としては「ＡＡ」以上の評価が望ましいといえます。重大度「CRITICAL」については早急な対策が必要です。また情報漏洩や攻撃者に有用な情報を与えてしまうような脆弱性が複数検出されました。 多くは直ちに緊急性のある脆弱性ではありませんが、これら脆弱性が複数組み合わされたり、サイバー攻撃者にとって有力な情報をもとに攻撃を行って

SEVERITY	CVSS	NAME
CRITICAL	10	KB4022715：Windows 10 Version 1607およびWindows Server 2016 June 2017累積更新
CRITICAL	10	KB4038782：Windows 10 Version 1607およびWindows Server 20162017年9月累積更新
CRITICAL	10	Microsoft Office Excel製品のセキュリティ更新プログラム（2017年9月）
CRITICAL	10	Microsoft Excel製品のセキュリティ更新プログラム（2017年11月）
CRITICAL	10	Microsoft Word製品のセキュリティ更新プログラム（2017年11月）
HIGH	9.4	.NET Frameworkのセキュリティと品質のロールアップ（2001年9月）
HIGH	9.3	MS15-124：Internet Explorerの累積的なセキュリティ更新プログラム（3116180）
HIGH	9.3	Windowsプリントスプーラのセキュリティ更新プログラム（3170005）
HIGH	9.3	Adobe Flash Player <= 26.0.0.137複数の脆弱性（APSB17-23）
HIGH	9.3	KB4034662：Adobe Flash Playerのセキュリティ更新プログラム（2001年8月）
HIGH	9.3	Google Chrome <61.0.3163.79複数の脆弱性
HIGH	9.3	Microsoft Publisher製品のセキュリティ更新プログラム（2017年9月）
HIGH	9.3	Adobe Flash Player <= 26.0.0.151複数の脆弱性（APSB17-28）
HIGH	9.3	Microsoft Powerpoint製品のセキュリティ更新プログラム（2017年9月）
HIGH	9.3	KB4038806：Adobe Flash Playerのセキュリティ更新プログラム（2011年9月）
HIGH	9.3	Google Chrome <61.0.3163.100複数の脆弱性
HIGH	9.3	Outlook用セキュリティ更新プログラム（2017年10月）
HIGH	9.3	Adobe Flash Player <= 27.0.0.159タイプ混乱の脆弱性（APSB17-32）
HIGH	9.3	Adobe Flash Playerのセキュリティ更新プログラム（October 2017）
HIGH	9.3	Google Chrome <62.0.3202.62複数の脆弱性
HIGH	9.3	Google Chrome <62.0.3202.89複数の脆弱性
HIGH	9.3	Google Chrome <63.0.3239.84複数の脆弱性
HIGH	9.3	Microsoft Office製品のセキュリティ更新プログラム（2017年12月）
HIGH	9.3	Google Chrome <63.0.3239.108複数の脆弱性
HIGH	9.3	Microsoft Excel製品のセキュリティ更新プログラム（2018年1月）
HIGH	9.3	Outlook用セキュリティ更新プログラム（2018年1月）
HIGH	9.3	Microsoft Word製品のセキュリティ更新プログラム（2018年1月）
HIGH	9.3	Microsoft Office製品のセキュリティ更新プログラム（2018年1月）
HIGH	9.3	Adobe Flash Player <= 28.0.0.137使用後フリー・リモート・コードの実行（APSA18-01）（APSB18-03）
HIGH	9.3	Adobe Flash Playerのセキュリティ更新プログラム（2018年2月）
HIGH	9.3	Microsoft Office製品のセキュリティ更新プログラム（2018年2月）
HIGH	9.3	Outlook用セキュリティ更新プログラム（2018年2月）
HIGH	9.3	Google Chrome <64.0.3282.167 V8JSFunction :: CalculateInstanceSizeForDerivedClass（）RCE
HIGH	9.3	Google Chrome <65.0.3325.146複数の脆弱性
HIGH	9.3	Microsoft Word製品のセキュリティ更新プログラム（2018年3月）
HIGH	7.6	KB4041691：Windows 10 Version 1607およびWindows Server 2016 October2017累積更新（KRACK）
HIGH	7.6	Microsoft Windows SMBサーバー（2017-10）の複数の脆弱性（非クレデンシャルチェック）

SEVERITY	CVSS	NAME
HIGH	7.6	KB4048953 : Windows 10 Version 1607およびWindows Server 2016 November2017累積的な更新
HIGH	7.6	KB4053579 : Windows 10 Version 1607およびWindows Server 2016 December2017年セキュリティアップデート
HIGH	7.6	KB4056890 : Windows 10 Version 1607およびWindows Server 2016 January2018セキュリティアップデート（メルトダウン）
HIGH	7.6	KB4074590 : Windows 10 Version 1607およびWindows Server 2016 February2018年セキュリティアップデート
HIGH	7.6	Adobe Flash Player <= 28.0.0.161（APSB18-05）
HIGH	7.6	Adobe Flash Playerのセキュリティ更新プログラム（2018年3月）
HIGH	7.6	KB4088787 : Windows 10 Version 1607およびWindows Server 2016 March2018年セキュリティアップデート
HIGH	7.2	.NET Frameworkのセキュリティと品質ロールアップ（2017年4月）
HIGH	7.2	KB4034658 : Windows 10 Version 1607およびWindows Server 2016 August2017累積的な更新
HIGH	7.2	Microsoft Office製品のセキュリティ更新プログラム（2017年9月）
HIGH	7.2	Microsoft Office製品のセキュリティ更新プログラム（2017年10月）
HIGH	7.2	Adobe Flash Player <= 27.0.0.183（APSB17-33）
HIGH	7.2	KB4048951 : Adobe Flash Playerのセキュリティ更新プログラム（2001年11月）
HIGH	7.2	Microsoft Office製品のセキュリティ更新プログラム（2017年11月）
HIGH	7.2	Adobe Flash Player <= 28.0.0.126（APSB18-01）
HIGH	7.1	KB4056887 : Adobe Flash Playerのセキュリティ更新プログラム（2018年1月）
HIGH	7.1	Google Chrome <62.0.3202.94範囲外V8での読み取りの不具合
HIGH	7.1	Google Chrome <64.0.3282.119複数の脆弱性
MEDIUM	6.9	Microsoft Windows引用符なしサービスパスの列挙
MEDIUM	6.8	Google Chrome <64.0.3282.140 V8 Factory :: NewFunction（）RCE
MEDIUM	5	.NET Frameworkのセキュリティと品質ロールアップ（2017年5月）
MEDIUM	5	Adobe Flash Player <= 27.0.0.187（APSB17-42）
MEDIUM	5	KB4053577 : Adobe Flash Playerのセキュリティ更新プログラム（2001年12月）192.168.1.2 7
MEDIUM	4.3	Microsoft Excel製品のセキュリティ更新プログラム（2018年3月）
MEDIUM	4	MS KB2960358 : .NET TLSでRC4を無効にするための更新
LOW	2.6	Microsoft Windows SMBレジストリ : Winlogonキャッシュされたパスワードの弱点

総評

【概要】
プラットフォーム脆弱性診断結果より、**緊急対応が必要な内容を含む重大なセキュリティの脆弱性が含まれて**おります。今回、「CRITICAL」と診断された脆弱性はWindows Serverにおける累積更新アップデートがなされていない事に関するもの、および「Microsoft Office Excel製品」に関する脆弱性についてになります。いずれもこのまま放置すると非常に深刻なサイバーセキュリティ上の事故を引き起こす恐れがあります。**早急に対策を検討し、脆弱性の対策を実施して下さい。**

【Microsoft WindowsOSの累積アップデートに関する脆弱性】
Microsoft WindowsOSにおけるセキュリティに関するアップデートがきちんとなされていないようです。
「KB4038782」は2017 年 9 月 13 日に配信されたアップデートで攻撃者が man-in-the-middle (MiTM) 攻撃をワークステーションやプリント サーバーに仕掛けたり、標的とするネットワーク上で非承認のプリント サーバーをセットアップしたりできる場合に、リモートでコードが実行される可能性などを修正したもので早急に、アップデートをしてください。

▽man-in-the-middle (MiTM) 攻撃 （中間者攻撃）
通常は無線LANや中継地点のネットワーク機器などに十分なセキュリティ対策が施されていない場合に発生するケースですが今回の脆弱性では感染したPCとネットワークでつながっている各種機器間通信を傍受される恐れがあります。身近なところではプリンターで出力した内容を傍受されると企業の機密情報が漏洩する恐れがあります。

▽リモートでコードが実行される可能性▽
文字通り、感染したPCを攻撃者がリモートで乗っ取ることが可能となります。乗っ取られたPCは、攻撃者が欲しい情報を漏洩させたり、またPCの権限を利用して（時には権限の昇格を行い）さらにネットワーク上の他端末に侵入します。

【Microsoft Office 製品に関する脆弱性について】
今回多く検出された脆弱性の中でMicrosoft Office 製品に関する脆弱性が見られました。これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生する可能性があります。全脆弱性64件中、16件含まれていました。

【サードパーティー製アプリケーションに関する脆弱性について】
上記以外、Adobe社製品に代表されるサードパーティー製品に関する脆弱性は、最もサイバー攻撃に利用される脆弱性の一つです。今回検出された全脆弱性64件中、16件含まれていました。

▽エクスプロイトキットによるマルウェア感染の可能性▽
エクスプロイトキット（別名：エクスプロイトパック）は、サイバー犯罪者が PC やデバイスの脆弱性を利用する際に用いるハッキングツールです。これにより不正プログラムの拡散やその他の不正活動が可能になります。
今回の診断結果で多くみられた、主に「Adobe Flash Player」や、「Java」、「Microsoft Silverlight」など、よく使用されるソフトウェアの脆弱性の典型例です。

マルウェアに感染すると身近なところでは以下の被害の恐れがあります。
・ランサムウェア
PCがこのマルウェアに感染すると、PC内またはPCが権限を持つ外部ストレージ内のデータが暗号化され身代金が要求されます。一度暗号化されたデータの複合化はほぼできません。また攻撃者の言いなりになって身代金を支払っても半数はデータがもとに戻らないという報告があります。

・オンライン銀行詐欺ツール
マルウェアによってオンライン銀行とのやりとりを傍受されたり偽のオンライン銀行に誘導され認証情報を抜き取られたりします。結果知らぬ間に攻撃者の用意した口座に不正送金が行われるケースが後を絶ちません。

Credential Scan Sample

CyberSecurityReport

Thu, 05 Apr 2018 12:01:39 JST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Remediations

Vulnerabilities by Plugin

103128 (2) - KB4038782: Windows 10 Version 1607 and Windows Server 2016 September 2017 Cumulative Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4038782.

It is, therefore, affected by multiple vulnerabilities :

- A race condition that could lead to a remote code execution vulnerability exists in NetBT Session Services when NetBT fails to maintain certain sequencing requirements. (CVE-2017-0161)

- A vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-11766)

- A spoofing vulnerability exists in Microsoft's implementation of the Bluetooth stack. An attacker who successfully exploited this vulnerability could perform a man-in-the-middle attack and force a user's computer to unknowingly route traffic through the attacker's computer. The attacker can then monitor and read the traffic before sending it on to the intended recipient.

(CVE-2017-8628)

- An information disclosure vulnerability exists when Microsoft Edge improperly handles clipboard events. For an attack to be successful, an attacker must persuade a user to visit a malicious website and leave it open during clipboard activities. The update addresses the vulnerability by changing how Microsoft Edge handles clipboard events in the browser. (CVE-2017-8643)

- An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.

(CVE-2017-8675)

- An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. (CVE-2017-8676)

- A information disclosure vulnerability exists when the Windows GDI+ component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2017-8677, CVE-2017-8681)

- A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.(CVE-2017-8682)

- An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.(CVE-2017-8683)

- A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server. An attacker who successfully exploited the vulnerability could either run arbitrary code on the DHCP failover server or cause the DHCP service to become nonresponsive.

(CVE-2017-8686)

- An Information disclosure vulnerability exists in Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass. An attacker who successfully exploited this vulnerability could retrieve the memory address of a kernel object.(CVE-2017-8687)

- An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface+ (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability.(CVE-2017-8688)

- A remote code execution vulnerability exists due to the way Windows Uniscribe handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2017-8692)

- An information disclosure vulnerability exists when Windows Uniscribe improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2017-8695)

- A remote code execution vulnerability exists when Windows Shell does not properly validate file copy destinations. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system.

(CVE-2017-8699)

- An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it.

An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality.

(CVE-2017-8702)

- A denial of service vulnerability exists when Microsoft Hyper-V Virtual PCI on a host server fails to properly validate input from a privileged user on a guest operating system.

input. (CVE-2017-8704)

- An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, allowing an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass. An attacker who successfully exploited this vulnerability could retrieve the base address of the kernel driver from a compromised process. (CVE-2017-8708)

- An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system.

(CVE-2017-8706, CVE-2017-8707, CVE-2017-8711, CVE-2017-8712, CVE-2017-8713)

- A remote code execution vulnerability exists in the VM Host Agent Service of Remote Desktop Virtual Host role when it fails to properly validate input from an authenticated user on a guest operating system.

(CVE-2017-8714)

- An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system. (CVE-2017-8678, CVE-2017-8679, CVE-2017-8709, CVE-2017-8719)

- An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs;

view, change, or delete data; or create new accounts with full user rights.(CVE-2017-8720)

- A spoofing vulnerability exists when Internet Explorer improperly handles specific HTML content. An attacker who successfully exploited this vulnerability could trick a user into believing that the user was visiting a legitimate website.

(CVE-2017-8733)

- A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-8731, CVE-2017-8734)

- A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services.

(CVE-2017-8735)

- An information disclosure vulnerability exists in Microsoft browsers due to improper parent domain verification in certain functionality. An attacker who successfully exploited the vulnerability could obtain specific information that is used in the parent domain.

(CVE-2017-8736)

- A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-8728, CVE-2017-8737)

- A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session.(CVE-2017-8746)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8649, CVE-2017-8660, CVE-2017-8741, CVE-2017-8748)

- A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8747, CVE-2017-8749)

- A remote code execution vulnerability exists when Microsoft browsers improperly access objects in memory.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.(CVE-2017-8750)

- A security feature bypass exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker who exploited the bypass could trick a user into loading a page containing malicious content.

(CVE-2017-8723, CVE-2017-8754)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-11764, CVE-2017-8738, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756)

- A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8757)

- A remote code execution vulnerability exists when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploited this vulnerability in software using the .NET framework could take control of an affected system.

(CVE-2017-8759)

See Also

http://www.nessus.org/u?62a3aab5

Solution

Apply security update KB4038782.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2017-0161
CVE	CVE-2017-11764
CVE	CVE-2017-11766
CVE	CVE-2017-8628

CVE	CVE-2017-8643
CVE	CVE-2017-8649
CVE	CVE-2017-8660
CVE	CVE-2017-8675
CVE	CVE-2017-8676
CVE	CVE-2017-8677
CVE	CVE-2017-8678
CVE	CVE-2017-8679
CVE	CVE-2017-8681
CVE	CVE-2017-8682
CVE	CVE-2017-8683
CVE	CVE-2017-8686
CVE	CVE-2017-8687
CVE	CVE-2017-8688
CVE	CVE-2017-8692
CVE	CVE-2017-8695
CVE	CVE-2017-8699
CVE	CVE-2017-8702
CVE	CVE-2017-8704
CVE	CVE-2017-8706
CVE	CVE-2017-8707
CVE	CVE-2017-8708
CVE	CVE-2017-8709
CVE	CVE-2017-8711
CVE	CVE-2017-8712
CVE	CVE-2017-8713
CVE	CVE-2017-8714
CVE	CVE-2017-8719
CVE	CVE-2017-8720
CVE	CVE-2017-8723
CVE	CVE-2017-8728
CVE	CVE-2017-8731
CVE	CVE-2017-8733
CVE	CVE-2017-8734
CVE	CVE-2017-8735
CVE	CVE-2017-8736
CVE	CVE-2017-8737
CVE	CVE-2017-8738
CVE	CVE-2017-8741
CVE	CVE-2017-8746
CVE	CVE-2017-8747
CVE	CVE-2017-8748
CVE	CVE-2017-8749

CVE	CVE-2017-8750
CVE	CVE-2017-8752
CVE	CVE-2017-8753
CVE	CVE-2017-8754
CVE	CVE-2017-8755
CVE	CVE-2017-8756
CVE	CVE-2017-8757
CVE	CVE-2017-8759
MSKB	4038782
XREF	MSFT:MS17-4038782

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information:

Published: 2017/09/12, Modified: 2018/03/02

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4038782

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1715
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4038782

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1737
```

20284 (1) - Kaspersky Anti-Virus Detection and Status

Synopsis

An antivirus application is installed on the remote host, but it is not working properly.

Description

Kaspersky Anti-Virus, a commercial antivirus software package for Windows, is installed on the remote host. However, there is a problem with the installation; either its services are not running or its engine and/or virus definitions are out of date.

See Also

http://www.kaspersky.com/

Solution

Make sure that updates are working and the associated services are running.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Published: 2005/12/09, Modified: 2017/09/05

Plugin Output

192.168.1.2 (tcp/445)

```
Kaspersky Anti-Virus is installed on the remote host :

  Product name      : Kaspersky Endpoint Security for Windows
  Version           : 10.2.5.3201
  Installation path : C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for
 Windows SP1\
  Virus signatures  : 09/09/2017

The virus signatures on the remote host are out-of-date - the last
known update from the vendor is 04/03/2018
```

```
As a result, the remote host might be infected by viruses.
```

100760 (1) - KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4022715. It is, therefore, affected by multiple vulnerabilities :

- Multiple security bypass vulnerabilities exist in Device Guard. A local attacker can exploit these, via a specially crafted script, to bypass the Device Guard Code Integrity policy and inject arbitrary code into a trusted PowerShell process. (CVE-2017-0173, CVE-2017-0215, CVE-2017-0216, CVE-2017-0218, CVE-2017-0219)

- An elevation of privilege vulnerability exists in Windows Hyper-V instruction emulation due to a failure to properly enforce privilege levels. An attacker on a guest operating system can exploit this to gain elevated privileges on the guest. Note that the host operating system is not vulnerable. (CVE-2017-0193)

- Multiple information disclosure vulnerabilities exist in Windows Uniscribe due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website or open a specially crafted document, to disclose the contents of memory. (CVE-2017-0282, CVE-2017-0284, CVE-2017-0285)

- A remote code execution vulnerability exists in Windows Uniscribe software due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website or to open a specially crafted document, to execute arbitrary code in the context of the current user. (CVE-2017-0283)

- Multiple information disclosure vulnerabilities exist in the Windows GDI component due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website or open a specially crafted document, to disclose the contents of memory.

(CVE-2017-0287, CVE-2017-0288, CVE-2017-0289, CVE-2017-8531, CVE-2017-8532, CVE-2017-8533)

- Multiple remote code execution vulnerabilities exist in Microsoft Windows due to improper parsing of PDF files.

An unauthenticated, remote attacker can exploit these, by convincing a user to open a specially crafted PDF file, to execute arbitrary code in the context of the current user. (CVE-2017-0291, CVE-2017-0292)

- A remote code execution vulnerability exists in Microsoft Windows due to improper handling of cabinet files. An unauthenticated, remote attacker can exploit this, by convincing a user to open a specially crafted cabinet file, to execute arbitrary code in the context of the current user. (CVE-2017-0294)

- A flaw exists in Microsoft Windows due to incorrect permissions being set on folders inside the DEFAULT folder structure. An authenticated, remote attacker can exploit this, by logging in to the affected system before the user can log in, to modify the user's DEFAULT folder contents. (CVE-2017-0295)

- An elevation of privilege vulnerability exists in tdx.sys due to a failure to check the length of a buffer prior to copying memory to it. A local attacker can exploit this, via a specially crafted application, to execute arbitrary code in an elevated context.

(CVE-2017-0296)

- An elevation of privilege vulnerability exists in the Windows kernel due to improper handling of objects in memory. A local attacker can exploit this, via a specially crafted application, to execute arbitrary code with elevated permissions. (CVE-2017-0297)

- An elevation of privilege vulnerability exists in the DCOM object in Helppane.exe, when configured to run as the interactive user, due to a failure to properly authenticate the client. An authenticated, remote attacker can exploit this, via a specially crafted application, to run arbitrary code in another user's session after that user has logged on to the same system using Terminal Services or Fast User Switching.

(CVE-2017-0298)

- Multiple information disclosure vulnerabilities exist in the Windows kernel due to improper initialization of objects in memory. An authenticated, remote attacker can exploit these, via a specially crafted application, to disclose the base address of the kernel driver.

(CVE-2017-0299, CVE-2017-0300, CVE-2017-8462, CVE-2017-8485)

- An information disclosure vulnerability exists in Microsoft Windows due to improper parsing of PDF files.

An unauthenticated, remote attacker can exploit this, by convincing a user to open a specially crafted PDF file, to disclose the contents of memory. (CVE-2017-8460)

- A remote code execution vulnerability exists in Windows due to improper handling of shortcuts. An unauthenticated, remote attacker can exploit this, by convincing a user to insert a removable drive containing a malicious shortcut and binary, to automatically execute arbitrary code in the context of the current user. (CVE-2017-8464)

- Multiple elevation of privilege vulnerabilities exist in the Windows kernel-mode driver due to improper handling of objects in memory. A local attacker can exploit these, via a specially crafted application, to run processes in an elevated context. (CVE-2017-8465, CVE-2017-8466, CVE-2017-8468)

- Multiple information disclosure vulnerabilities exist in the Windows kernel due to improper initialization of objects in memory. An authenticated, remote attacker can exploit these, via a specially crafted application, to disclose sensitive information. (CVE-2017-8470, CVE-2017-8471, CVE-2017-8473, CVE-2017-8474, CVE-2017-8475, CVE-2017-8476, CVE-2017-8477, CVE-2017-8478, CVE-2017-8479, CVE-2017-8480, CVE-2017-8481, CVE-2017-8482, CVE-2017-8483, CVE-2017-8484, CVE-2017-8489, CVE-2017-8490, CVE-2017-8491, CVE-2017-8492)

- A security bypass vulnerability exists due to a failure to enforce case sensitivity for certain variable checks.

A local attacker can exploit this, via a specially crafted application, to bypass Unified Extensible Firmware Interface (UEFI) variable security.

(CVE-2017-8493)

- An elevation of privilege vulnerability exists in the Windows Secure Kernel Mode feature due to a failure to properly handle objects in memory. A local attacker can exploit this, via a specially crafted application, to bypass virtual trust levels (VTL). (CVE-2017-8494)

- Multiple remote code execution vulnerabilities exist in Microsoft Edge due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8496, CVE-2017-8497)

- An information disclosure vulnerability exists in Microsoft Edge due to improper handling of JavaScript XML DOM objects. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to disclose sensitive information.

(CVE-2017-8498)

- An information disclosure vulnerability exists in Microsoft Edge in the Fetch API due to improper handling of filtered response types. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to disclose sensitive information in the URL of a cross-origin request.

(CVE-2017-8504)

- A denial of service vulnerability exists in Windows due to improper handling of kernel mode requests. An unauthenticated, remote attacker can exploit this, via a specially crafted kernel mode request, to cause the machine to stop responding or rebooting. (CVE-2017-8515)

- Multiple remote code execution vulnerabilities exist in Microsoft browsers in the JavaScript engines due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8517, CVE-2017-8522, CVE-2017-8524, CVE-2017-8548)

- A same-origin policy bypass vulnerability exists in Microsoft Edge due to a failure to properly apply the Same Origin Policy for HTML elements. An unauthenticated, remote attacker can exploit this, by convincing a user to follow a link, to load a page with malicious content. (CVE-2017-8523)

- A remote code execution vulnerability exists in the Windows font library due to improper handling of embedded fonts. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website or open a specially crafted Microsoft document, to execute arbitrary code in the context of the current user. (CVE-2017-8527)

- An information disclosure vulnerability exists in Microsoft browsers in the scripting engines due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to disclose files on a user's computer. (CVE-2017-8529)*

- A same-origin policy bypass vulnerability exists in Microsoft Edge due to a failure to properly enforce same-origin policies. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to disclose information from origins outside the current one. (CVE-2017-8530)

- A remote code execution vulnerability exists in the Windows Search functionality due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, via a specially crafted SMB message, to execute arbitrary code. (CVE-2017-8543)

- An information disclosure vulnerability exists in the Windows Search functionality due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, via a specially crafted SMB message, to disclose sensitive information. (CVE-2017-8544)

- A remote code execution vulnerability exists in Internet Explorer due to improper handling of objects in memory.

An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8547)

- A remote code execution vulnerability exists in Microsoft Edge in the JavaScript scripting engine due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8549)

- Multiple information disclosure vulnerabilities exist in the Windows kernel due to improper handling of objects in memory. An authenticated, remote attacker can exploit these, via a specially crafted application, to disclose the contents of memory. (CVE-2017-8553, CVE-2017-8554)

- An information disclosure vulnerability exists in the Windows Graphics component due to improper handling of objects in memory. An authenticated, remote attacker can exploit this, via a specially crafted application, to disclose sensitive information. (CVE-2017-8575)

- An elevation of privilege vulnerability exists in the Windows Graphics component due to improper initialization of objects in memory. A local attacker can exploit this, via a specially crafted application, to execute arbitrary code in kernel mode.

(CVE-2017-8576)

- An elevation of privilege vulnerability exists DirectX due to improper handling of objects in memory. A local attacker can exploit this, via a specially crafted application, to execute arbitrary code in kernel mode.

(CVE-2017-8576)

* note that a registry value must be added to enable the fix for CVE-2017-8529. if the patch is installed but not enabled, the registry key needed will be detailed in the output below.

See Also

http://www.nessus.org/u?4ac6572f

http://www.nessus.org/u?1f6a3c24

Solution

Apply security update KB4022715.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	98818
BID	98819
BID	98820
BID	98821
BID	98824
BID	98826

BID	98833
BID	98835
BID	98836
BID	98837
BID	98839
BID	98840
BID	98843
BID	98844
BID	98845
BID	98846
BID	98847
BID	98848
BID	98849
BID	98850
BID	98852
BID	98853
BID	98854
BID	98855
BID	98856
BID	98857
BID	98858
BID	98859
BID	98860
BID	98862
BID	98863
BID	98865
BID	98867
BID	98869
BID	98870
BID	98873
BID	98878
BID	98879
BID	98880
BID	98882
BID	98884
BID	98885
BID	98886
BID	98887
BID	98892
BID	98895
BID	98896
BID	98897
BID	98898

BID	98900
BID	98901
BID	98902
BID	98903
BID	98904
BID	98914
BID	98918
BID	98920
BID	98922
BID	98923
BID	98926
BID	98928
BID	98929
BID	98930
BID	98932
BID	98933
BID	98940
BID	98942
BID	98953
BID	98954
BID	98955
BID	99210
BID	99212
BID	99215
CVE	CVE-2017-0173
CVE	CVE-2017-0193
CVE	CVE-2017-0215
CVE	CVE-2017-0216
CVE	CVE-2017-0218
CVE	CVE-2017-0219
CVE	CVE-2017-0282
CVE	CVE-2017-0283
CVE	CVE-2017-0284
CVE	CVE-2017-0285
CVE	CVE-2017-0287
CVE	CVE-2017-0288
CVE	CVE-2017-0289
CVE	CVE-2017-0291
CVE	CVE-2017-0292
CVE	CVE-2017-0294
CVE	CVE-2017-0295
CVE	CVE-2017-0296
CVE	CVE-2017-0297

CVE	CVE-2017-0298
CVE	CVE-2017-0299
CVE	CVE-2017-0300
CVE	CVE-2017-8460
CVE	CVE-2017-8462
CVE	CVE-2017-8464
CVE	CVE-2017-8465
CVE	CVE-2017-8466
CVE	CVE-2017-8468
CVE	CVE-2017-8470
CVE	CVE-2017-8471
CVE	CVE-2017-8473
CVE	CVE-2017-8474
CVE	CVE-2017-8475
CVE	CVE-2017-8476
CVE	CVE-2017-8477
CVE	CVE-2017-8478
CVE	CVE-2017-8479
CVE	CVE-2017-8480
CVE	CVE-2017-8481
CVE	CVE-2017-8482
CVE	CVE-2017-8483
CVE	CVE-2017-8484
CVE	CVE-2017-8485
CVE	CVE-2017-8489
CVE	CVE-2017-8490
CVE	CVE-2017-8491
CVE	CVE-2017-8492
CVE	CVE-2017-8493
CVE	CVE-2017-8494
CVE	CVE-2017-8496
CVE	CVE-2017-8497
CVE	CVE-2017-8498
CVE	CVE-2017-8504
CVE	CVE-2017-8515
CVE	CVE-2017-8517
CVE	CVE-2017-8518
CVE	CVE-2017-8522
CVE	CVE-2017-8523
CVE	CVE-2017-8524
CVE	CVE-2017-8527
CVE	CVE-2017-8529
CVE	CVE-2017-8530

CVE	CVE-2017-8531
CVE	CVE-2017-8532
CVE	CVE-2017-8533
CVE	CVE-2017-8543
CVE	CVE-2017-8544
CVE	CVE-2017-8547
CVE	CVE-2017-8548
CVE	CVE-2017-8549
CVE	CVE-2017-8553
CVE	CVE-2017-8575
CVE	CVE-2017-8576
CVE	CVE-2017-8579
CVE	CVE-2017-8554
MSKB	4022715
XREF	OSVDB:158914
XREF	OSVDB:158917
XREF	OSVDB:158918
XREF	OSVDB:158919
XREF	OSVDB:158920
XREF	OSVDB:158921
XREF	OSVDB:158922
XREF	OSVDB:158923
XREF	OSVDB:158924
XREF	OSVDB:158926
XREF	OSVDB:158927
XREF	OSVDB:158929
XREF	OSVDB:158930
XREF	OSVDB:158931
XREF	OSVDB:158932
XREF	OSVDB:158933
XREF	OSVDB:158934
XREF	OSVDB:158935
XREF	OSVDB:158936
XREF	OSVDB:158940
XREF	OSVDB:158941
XREF	OSVDB:158942
XREF	OSVDB:158947
XREF	OSVDB:158948
XREF	OSVDB:158949
XREF	OSVDB:158950
XREF	OSVDB:158951
XREF	OSVDB:158953
XREF	OSVDB:158954

XREF OSVDB:158955
XREF OSVDB:158956
XREF OSVDB:158957
XREF OSVDB:158959
XREF OSVDB:158960
XREF OSVDB:158961
XREF OSVDB:158962
XREF OSVDB:158963
XREF OSVDB:158964
XREF OSVDB:158965
XREF OSVDB:158966
XREF OSVDB:158967
XREF OSVDB:158968
XREF OSVDB:158970
XREF OSVDB:158972
XREF OSVDB:158973
XREF OSVDB:158974
XREF OSVDB:158975
XREF OSVDB:158976
XREF OSVDB:158977
XREF OSVDB:158978
XREF OSVDB:158979
XREF OSVDB:158980
XREF OSVDB:158981
XREF OSVDB:158982
XREF OSVDB:158983
XREF OSVDB:158984
XREF OSVDB:158985
XREF OSVDB:158986
XREF OSVDB:158987
XREF OSVDB:158996
XREF OSVDB:158998
XREF OSVDB:158999
XREF OSVDB:159000
XREF OSVDB:159001
XREF OSVDB:159002
XREF OSVDB:159003
XREF OSVDB:159004
XREF OSVDB:159005
XREF OSVDB:159006
XREF OSVDB:159007
XREF OSVDB:159612
XREF OSVDB:159613

XREF	OSVDB:159614
XREF	OSVDB:159999
XREF	MSFT:MS17-4022715

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information:

Published: 2017/06/13, Modified: 2018/03/19

Plugin Output

192.168.1.2 (tcp/445)

```
  The following registry key is missing.This registry key is required to enable the fix for
 CVE-2017-8529:
  SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX
\iexplore.exe

the following registry key is missing.This registry key is required to enable the fix for
 cve-2017-8529:
  SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl
\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe
```

103138 (1) - Security Update for Microsoft Office Excel Products (September 2017)

Synopsis

The Microsoft Excel Products are affected by multiple vulnerabilities.

Description

The Microsoft Excel Products are missing security updates.

It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory.

(CVE-2017-8631, CVE-2017-8632)

See Also

http://www.nessus.org/u?9d426bc7

http://www.nessus.org/u?b2583452

http://www.nessus.org/u?8028c458

http://www.nessus.org/u?7194ec3f

Solution

Microsoft has released the following security updates to address this issue:

-KB4011108

-KB4011050

-KB4011061

-KB4011062

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	100734
BID	100751
CVE	CVE-2017-8631
CVE	CVE-2017-8632
MSKB	4011050
MSKB	4011108
MSKB	4011062
MSKB	4011061
XREF	OSVDB:165292
XREF	OSVDB:165293
XREF	MSFT:MS17-4011050
XREF	MSFT:MS17-4011108
XREF	MSFT:MS17-4011062
XREF	MSFT:MS17-4011061
XREF	IAVA:2017-A-0274

Plugin Information:

Published: 2017/09/12, Modified: 2017/09/15

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Excel 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe has not been patched.
  Remote version    : 14.0.7183.5000
  Fixed version     : 14.0.7188.5000
```

104556 (1) - Security Updates for Microsoft Excel Products (November 2017)

Synopsis

The Microsoft Excel Products are affected by multiple vulnerabilities.

Description

The Microsoft Excel Products are missing security updates.

It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-11878)

- A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run.

(CVE-2017-11877)

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. (CVE-2017-11884)

See Also

http://www.nessus.org/u?92b81e09

http://www.nessus.org/u?ec4b4942

http://www.nessus.org/u?79b55073

http://www.nessus.org/u?c66f32ec

Solution

Microsoft has released the following security updates to address this issue:

-KB4011197

-KB4011220

-KB4011233

-KB4011199

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	100734
BID	100751
BID	101766
CVE	CVE-2017-11877
CVE	CVE-2017-11878
CVE	CVE-2017-11884
MSKB	4011197
MSKB	4011220
MSKB	4011233
MSKB	4011199
XREF	OSVDB:169254
XREF	OSVDB:169256
XREF	OSVDB:169257
XREF	MSFT:MS17-4011197
XREF	MSFT:MS17-4011220
XREF	MSFT:MS17-4011233
XREF	MSFT:MS17-4011199
XREF	IAVA:2017-A-0337

Plugin Information:

Published: 2017/11/14, Modified: 2017/11/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Excel 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe has not been patched.
  Remote version    : 14.0.7183.5000
  Fixed version     : 14.0.7190.5000
```

104562 (1) - Security Updates for Microsoft Word Products (November 2017)

Synopsis

The Microsoft Word Products are missing a security update.

Description

The Microsoft Office Products are missing a security update.

It is, therefore, affected by the following vulnerability :

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-11854)

See Also

http://www.nessus.org/u?7e369ce9

http://www.nessus.org/u?f5d2afcd

http://www.nessus.org/u?10501d2c

http://www.nessus.org/u?dc04b98c

Solution

Microsoft has released the following security updates to address this issue:

-KB4011250

-KB4011242

-KB4011270

-KB4011266

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	101746
CVE	CVE-2017-11854
MSKB	4011250
MSKB	4011242
MSKB	4011270
MSKB	4011266
XREF	OSVDB:169235
XREF	MSFT:MS17-4011250
XREF	MSFT:MS17-4011242
XREF	MSFT:MS17-4011270
XREF	MSFT:MS17-4011266
XREF	IAVA:2017-A-0337

Plugin Information:

Published: 2017/11/14, Modified: 2017/11/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Word 2010
- C:\Program Files (x86)\Microsoft Office\Office14\WinWord.exe has not been patched.
  Remote version    : 14.0.7182.5000
  Fixed version     : 14.0.7190.5000
```

104549 (3) - KB4048953: Windows 10 Version 1607 and Windows Server 2016 November 2017 Cumulative Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4048953.

It is, therefore, affected by multiple vulnerabilities :

- A security feature bypass vulnerability exists when Microsoft Edge improperly handles redirect requests. The vulnerability allows Microsoft Edge to bypass Cross- Origin Resource Sharing (CORS) redirect restrictions, and to follow redirect requests that should otherwise be ignored. An attacker who successfully exploited the vulnerability could force the browser to send data that would otherwise be restricted to a destination website of the attacker's choice. (CVE-2017-11872)

- A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11827, CVE-2017-11858)

- A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-11837, CVE-2017-11838, CVE-2017-11843, CVE-2017-11846)

- A security feature bypass exists when Device Guard incorrectly validates an untrusted file. An attacker who successfully exploited this vulnerability could make an unsigned file appear to be signed. Because Device Guard relies on the signature to determine the file is non- malicious, Device Guard could then allow a malicious file to execute. In an attack scenario, an attacker could make an untrusted file appear to be a trusted file. The update addresses the vulnerability by correcting how Device Guard handles untrusted files.

(CVE-2017-11830)

- An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Internet Explorer. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2017-11834)

- A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11855, CVE-2017-11856, CVE-2017-11869)

- An information vulnerability exists when Windows Media Player improperly discloses file information. Successful exploitation of the vulnerability could allow the attacker to test for the presence of files on disk.

(CVE-2017-11768)

- An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.

(CVE-2017-11880)

- A security feature bypass vulnerability exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker who exploited the bypass could trick a user into loading a page containing malicious content. (CVE-2017-11863)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11836, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11861, CVE-2017-11866, CVE-2017-11873)

- A Win32k information disclosure vulnerability exists when the Windows GDI component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-11851)

- An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2017-11791)

- An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-11847)

- An information disclosure vulnerability exists when Internet Explorer improperly handles page content, which could allow an attacker to detect the navigation of the user leaving a maliciously crafted page.

(CVE-2017-11848)

- An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system. (CVE-2017-11831, CVE-2017-11842, CVE-2017-11849, CVE-2017-11853)

- A denial of service vulnerability exists when Windows Search improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a remote denial of service against a system.

(CVE-2017-11788)

- An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-11850)

- An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests.

An attacker who successfully exploited this vulnerability could determine the origin of all webpages in the affected browser. (CVE-2017-11833)

See Also

http://www.nessus.org/u?119c56db

Solution

Apply security update KB4048953.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	101703
BID	101705
BID	101706
BID	101709
BID	101711
BID	101714
BID	101715
BID	101716
BID	101719
BID	101721
BID	101722
BID	101723
BID	101725
BID	101727
BID	101728
BID	101729
BID	101732
BID	101733
BID	101734
BID	101735
BID	101737
BID	101738
BID	101740
BID	101741
BID	101742
BID	101748

BID	101749
BID	101751
BID	101753
BID	101755
BID	101762
BID	101763
BID	101764
CVE	CVE-2017-11768
CVE	CVE-2017-11788
CVE	CVE-2017-11791
CVE	CVE-2017-11827
CVE	CVE-2017-11830
CVE	CVE-2017-11831
CVE	CVE-2017-11833
CVE	CVE-2017-11834
CVE	CVE-2017-11836
CVE	CVE-2017-11837
CVE	CVE-2017-11838
CVE	CVE-2017-11839
CVE	CVE-2017-11840
CVE	CVE-2017-11841
CVE	CVE-2017-11842
CVE	CVE-2017-11843
CVE	CVE-2017-11846
CVE	CVE-2017-11847
CVE	CVE-2017-11848
CVE	CVE-2017-11849
CVE	CVE-2017-11850
CVE	CVE-2017-11851
CVE	CVE-2017-11853
CVE	CVE-2017-11855
CVE	CVE-2017-11856
CVE	CVE-2017-11858
CVE	CVE-2017-11861
CVE	CVE-2017-11863
CVE	CVE-2017-11866
CVE	CVE-2017-11869
CVE	CVE-2017-11872
CVE	CVE-2017-11873
CVE	CVE-2017-11880
MSKB	4048953
XREF	OSVDB:169209
XREF	OSVDB:169210

XREF	OSVDB:169211
XREF	OSVDB:169212
XREF	OSVDB:169213
XREF	OSVDB:169216
XREF	OSVDB:169217
XREF	OSVDB:169218
XREF	OSVDB:169219
XREF	OSVDB:169220
XREF	OSVDB:169221
XREF	OSVDB:169222
XREF	OSVDB:169223
XREF	OSVDB:169224
XREF	OSVDB:169227
XREF	OSVDB:169229
XREF	OSVDB:169230
XREF	OSVDB:169231
XREF	OSVDB:169233
XREF	OSVDB:169234
XREF	OSVDB:169238
XREF	OSVDB:169239
XREF	OSVDB:169240
XREF	OSVDB:169241
XREF	OSVDB:169242
XREF	OSVDB:169243
XREF	OSVDB:169244
XREF	OSVDB:169247
XREF	OSVDB:169250
XREF	OSVDB:169252
XREF	OSVDB:169253
XREF	OSVDB:169258
XREF	OSVDB:169259
XREF	MSFT:MS17-4048953

Plugin Information:

Published: 2017/11/14, Modified: 2017/12/18

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4048953

C:\Windows\system32\ntoskrnl.exe has not been patched.
```

```
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1797
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4048953

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1914
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4048953

C:\Windows\system32\win32kfull.sys has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1884
```

92018 (2) - MS16-087: Security Update for Windows Print Spooler (3170005)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing a security update. It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in the Windows Print Spooler service due to improper validation of print drivers while installing a printer from network servers. An unauthenticated, remote attacker can exploit this vulnerability, via a man-in-the-middle attack on a workstation or print server or via a rogue print server, to execute arbitrary code in the context of the current user. (CVE-2016-3238)

- An elevation of privilege vulnerability exists in the Windows Print Spooler service due to improperly allowing arbitrary writing to the file system. An attacker can exploit this issue, via a specially crafted script or application, to execute arbitrary code with elevated system privileges. (CVE-2016-3239)

See Also

https://technet.microsoft.com/library/security/MS16-087

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

II

References

BID	91609
BID	91612
CVE	CVE-2016-3238
CVE	CVE-2016-3239
MSKB	3170455
MSKB	4038777
MSKB	4038779
MSKB	4038781
MSKB	4038782
MSKB	4038783
MSKB	4038786
MSKB	4038792
MSKB	4038793
MSKB	4038799
XREF	OSVDB:141403
XREF	OSVDB:141404
XREF	MSFT:MS16-087
XREF	IAVA:2016-A-0181

Plugin Information:

Published: 2016/07/12, Modified: 2017/11/28

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4038782

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1715
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4038782

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1737
```

102264 (2) - KB4034658: Windows 10 Version 1607 and Windows Server 2016 August 2017 Cumulative Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4034658.

It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists when Microsoft Windows improperly handles NetBIOS packets. An attacker who successfully exploited this vulnerability could cause a target computer to become completely unresponsive. A remote unauthenticated attacker could exploit this vulnerability by sending a series of TCP packets to a target system, resulting in a permanent denial of service condition. The update addresses the vulnerability by correcting how the Windows network stack handles NetBIOS traffic. (CVE-2017-0174)

- A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2017-0250)

- A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-0293)

- An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser. An attacker who successfully exploited this vulnerability could gain elevated privileges and break out of the Edge AppContainer sandbox.The vulnerability by itself does not allow arbitrary code to run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (for example a remote code execution vulnerability and another elevation of privilege vulnerability) to take advantage of the elevated privileges when running.The security update addresses the vulnerability by modifying how Microsoft Edge handles sandboxing. (CVE-2017-8503)

- A remote code execution vulnerability exists in Windows Input Method Editor (IME) when IME improperly handles parameters in a method of a DCOM class. The DCOM server is a Windows component installed regardless of which languages/IMEs are enabled. An attacker can instantiate the DCOM class and exploit the system even if IME is not enabled. (CVE-2017-8591)

- An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs;

view, change, or delete data; or create new accounts with full user rights. (CVE-2017-8593)

- A remote code execution vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger

the vulnerability through an SMB connection and then take control of a target computer.The security update addresses the vulnerability by correcting how Windows Search handles objects in memory. (CVE-2017-8620)

- A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash. (CVE-2017-8623)

- An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory.(CVE-2017-8624)

- A security feature bypass vulnerability exists when Internet Explorer fails to validate User Mode Code Integrity (UMCI) policies. The vulnerability could allow an attacker to bypass Device Guard UCMI policies.To exploit the vulnerability, a user could either visit a malicious website or an attacker with access to the system could run a specially crafted application. An attacker could then leverage the vulnerability to run unsigned malicious code as though it were signed by a trusted source.The update addresses the vulnerability by correcting how Internet Explorer validates UMCI policies. (CVE-2017-8625)

- This security update resolves a vulnerability in Windows Error Reporting (WER). The vulnerability could allow elevation of privilege if successfully exploited by an attacker. An attacker who successfully exploited this vulnerability could gain greater access to sensitive information and system functionality. This update corrects the way the WER handles and executes files.

(CVE-2017-8633)

- A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8635)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8636)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8639)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8640)

- A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8641)

- An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-8644)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8645)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8646)

- An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-8652)

- A remote code execution vulnerability exists when Microsoft browsers improperly access objects in memory.

The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8653)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8655)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8656)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8657)

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8661)

- A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. (CVE-2017-8664)

- An information disclosure vulnerability exists when the win32k component improperly provides kernel information.

An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-8666)

- A remote code execution vulnerability exists in the way Microsoft browsers handle objects in memory while rendering content. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-8669)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8670)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8671)

- A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8672)

See Also

http://www.nessus.org/u?8b993cd6

Solution

Apply security update KB4034658.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	98100
BID	99395
BID	99430
BID	100027
BID	100032
BID	100033
BID	100034
BID	100035
BID	100037
BID	100038
BID	100039
BID	100042
BID	100044
BID	100047
BID	100050
BID	100051
BID	100052
BID	100053

BID	100055
BID	100056
BID	100057
BID	100059
BID	100061
BID	100063
BID	100068
BID	100069
BID	100070
BID	100071
BID	100072
BID	100085
BID	100089
CVE	CVE-2017-0174
CVE	CVE-2017-0250
CVE	CVE-2017-0293
CVE	CVE-2017-8503
CVE	CVE-2017-8591
CVE	CVE-2017-8593
CVE	CVE-2017-8620
CVE	CVE-2017-8623
CVE	CVE-2017-8624
CVE	CVE-2017-8625
CVE	CVE-2017-8633
CVE	CVE-2017-8635
CVE	CVE-2017-8636
CVE	CVE-2017-8639
CVE	CVE-2017-8640
CVE	CVE-2017-8641
CVE	CVE-2017-8644
CVE	CVE-2017-8645
CVE	CVE-2017-8646
CVE	CVE-2017-8652
CVE	CVE-2017-8653
CVE	CVE-2017-8655
CVE	CVE-2017-8656
CVE	CVE-2017-8657
CVE	CVE-2017-8661
CVE	CVE-2017-8664
CVE	CVE-2017-8666
CVE	CVE-2017-8669
CVE	CVE-2017-8670
CVE	CVE-2017-8671

CVE	CVE-2017-8672
MSKB	4034658
XREF	OSVDB:162747
XREF	OSVDB:162748
XREF	OSVDB:162749
XREF	OSVDB:162750
XREF	OSVDB:162761
XREF	OSVDB:162780
XREF	OSVDB:162805
XREF	OSVDB:162833
XREF	OSVDB:162841
XREF	OSVDB:162842
XREF	OSVDB:162846
XREF	OSVDB:162847
XREF	OSVDB:162848
XREF	OSVDB:162849
XREF	OSVDB:162853
XREF	OSVDB:162854
XREF	OSVDB:162855
XREF	OSVDB:162857
XREF	OSVDB:162859
XREF	OSVDB:162860
XREF	OSVDB:162861
XREF	OSVDB:162862
XREF	OSVDB:162863
XREF	OSVDB:162864
XREF	OSVDB:162865
XREF	OSVDB:162867
XREF	OSVDB:162871
XREF	OSVDB:162872
XREF	OSVDB:162876
XREF	OSVDB:162878
XREF	OSVDB:162879
XREF	MSFT:MS17-4034658

Plugin Information:

Published: 2017/08/08, Modified: 2017/11/28

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
```

```
  - 4034658

C:\Windows\System32\shell32.dll has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1593
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4034658

C:\Windows\System32\shell32.dll has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1596
```

103749 (2) - KB4041691: Windows 10 Version 1607 and Windows Server 2016 October 2017 Cumulative Update (KRACK)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4041691.

It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system. (CVE-2017-11765, CVE-2017-11814)

- An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions. An attacker who successfully exploited the vulnerability could overwrite files that require higher privileges than what the attacker already has. (CVE-2017-11829)

- A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-11762, CVE-2017-11763)

- An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2017-11783)

- A remote code execution vulnerability exists in Windows Domain Name System (DNS) DNSAPI.dll when it fails to properly handle DNS responses. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. (CVE-2017-11779)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11802, CVE-2017-11804, CVE-2017-11808, CVE-2017-11811, CVE-2017-11812)

- A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2017-8717, CVE-2017-8718)

- A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.

(CVE-2017-11823, CVE-2017-8715)

- An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.

(CVE-2017-11817)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-11793, CVE-2017-11810)

- An elevation of privilege vulnerability exists in the default Windows SMB Server configuration which allows anonymous users to remotely access certain named pipes that are also configured to allow anonymous access to users who are logged on locally. An unauthenticated attacker who successfully exploits this configuration error could remotely send specially crafted requests to certain services that accept requests via named pipes.

(CVE-2017-11782)

- An Information disclosure vulnerability exists when Windows Search improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-11772)

- An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2017-11824)

- A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory via the Microsoft Windows Text Services Framework. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8727)

- An Security Feature bypass vulnerability exists in Microsoft Windows storage when it fails to validate an integrity-level check. An attacker who successfully exploited the vulnerability could allow an application with a certain integrity level to execute code at a different integrity level. The update addresses the vulnerability by correcting how Microsoft storage validates an integrity-level check. (CVE-2017-11818)

- A remote code execution vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2017-11771)

- An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests. An authenticated attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server. (CVE-2017-11815)

- A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server. An attacker who exploited this vulnerability could cause the affected system to crash. To attempt to exploit this issue, an attacker would need to send specially crafted SMB requests to the target system. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests. The security update addresses the vulnerability by correcting the manner in which SMB handles specially crafted client requests.

(CVE-2017-11781)

- An elevation of privilege vulnerability exists when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs;

view, change, or delete data; or create new accounts with full user rights. (CVE-2017-8689, CVE-2017-8694)

- A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.

(CVE-2017-11780)

- An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-8693)

- An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. (CVE-2017-11816)

- A remote code execution vulnerability exists in the way the scripting engine handle objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-11809)

- An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. (CVE-2017-11785)

- A remote code execution vulnerability exists in the way that certain Windows components handle the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2017-11769)

- A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8726)

- An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.

An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-11790)

- A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11822)

- A spoofing vulnerability exists in the Windows implementation of wireless networking. An attacker who successfully exploited this vulnerability could potentially replay broadcast and/or multicast traffic to hosts on a WPA or WPA 2-protected wireless network.

(CVE-2017-13080)

See Also

http://www.nessus.org/u?62ef3ec8

Solution

Apply security update KB4041691.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:ND)

STIG Severity

II

References

BID	101077
BID	101081
BID	101084
BID	101093
BID	101094
BID	101095
BID	101096
BID	101099
BID	101100
BID	101101
BID	101102
BID	101108
BID	101109
BID	101110
BID	101111
BID	101112
BID	101114
BID	101116
BID	101122

BID	101125
BID	101126
BID	101127
BID	101128
BID	101130
BID	101131
BID	101135
BID	101136
BID	101137
BID	101138
BID	101139
BID	101140
BID	101141
BID	101142
BID	101143
BID	101144
BID	101149
BID	101161
BID	101162
BID	101163
BID	101166
BID	101213
BID	101274
CVE	CVE-2017-11762
CVE	CVE-2017-11763
CVE	CVE-2017-11765
CVE	CVE-2017-11769
CVE	CVE-2017-11771
CVE	CVE-2017-11772
CVE	CVE-2017-11779
CVE	CVE-2017-11780
CVE	CVE-2017-11781
CVE	CVE-2017-11782
CVE	CVE-2017-11783
CVE	CVE-2017-11785
CVE	CVE-2017-11790
CVE	CVE-2017-11793
CVE	CVE-2017-11798
CVE	CVE-2017-11799
CVE	CVE-2017-11800
CVE	CVE-2017-11802
CVE	CVE-2017-11804
CVE	CVE-2017-11808

CVE	CVE-2017-11809
CVE	CVE-2017-11810
CVE	CVE-2017-11811
CVE	CVE-2017-11812
CVE	CVE-2017-11814
CVE	CVE-2017-11815
CVE	CVE-2017-11816
CVE	CVE-2017-11817
CVE	CVE-2017-11818
CVE	CVE-2017-11822
CVE	CVE-2017-11823
CVE	CVE-2017-11824
CVE	CVE-2017-11829
CVE	CVE-2017-13080
CVE	CVE-2017-8689
CVE	CVE-2017-8693
CVE	CVE-2017-8694
CVE	CVE-2017-8715
CVE	CVE-2017-8717
CVE	CVE-2017-8718
CVE	CVE-2017-8726
CVE	CVE-2017-8727
MSKB	4041691
XREF	OSVDB:167038
XREF	OSVDB:167040
XREF	OSVDB:167041
XREF	OSVDB:167042
XREF	OSVDB:167043
XREF	OSVDB:167047
XREF	OSVDB:167048
XREF	OSVDB:167049
XREF	OSVDB:167051
XREF	OSVDB:167052
XREF	OSVDB:167053
XREF	OSVDB:167054
XREF	OSVDB:167055
XREF	OSVDB:167056
XREF	OSVDB:167057
XREF	OSVDB:167058
XREF	OSVDB:167059
XREF	OSVDB:167063
XREF	OSVDB:167064
XREF	OSVDB:167066

XREF	OSVDB:167067
XREF	OSVDB:167068
XREF	OSVDB:167070
XREF	OSVDB:167072
XREF	OSVDB:167073
XREF	OSVDB:167074
XREF	OSVDB:167075
XREF	OSVDB:167078
XREF	OSVDB:167079
XREF	OSVDB:167080
XREF	OSVDB:167083
XREF	OSVDB:167085
XREF	OSVDB:167087
XREF	OSVDB:167088
XREF	OSVDB:167089
XREF	OSVDB:167090
XREF	OSVDB:167095
XREF	OSVDB:167096
XREF	OSVDB:167097
XREF	OSVDB:167098
XREF	OSVDB:167099
XREF	OSVDB:167351
XREF	IAVA:2017-A-0310
XREF	MSFT:MS17-4041691

Plugin Information:

Published: 2017/10/10, Modified: 2017/12/21

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4041691

C:\Windows\system32\shell32.dll has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1770
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4041691

C:\Windows\system32\shell32.dll has not been patched.
```

```
      Remote version : 10.0.14393.1480
      Should be      : 10.0.14393.1794
```

106796 (2) - KB4074590: Windows 10 Version 1607 and Windows Server 2016 February 2018 Security Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4074590. It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2018-0866)

- An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system. (CVE-2018-0757, CVE-2018-0829, CVE-2018-0830)

- A remote code execution vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited these vulnerabilities could take control of an affected system. (CVE-2018-0842)

- A remote code execution vulnerability exists in StructuredQuery when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2018-0825)

- An elevation of privilege vulnerability exists when Storage Services improperly handles objects in memory.

An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2018-0826)

- An elevation of privilege vulnerability exists when NTFS improperly handles objects. An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2018-0822)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2018-0834, CVE-2018-0835, CVE-2018-0837, CVE-2018-0838, CVE-2018-0857, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861)

- An elevation of privilege vulnerability exists when AppContainer improperly implements constrained impersonation. An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2018-0821)

- An elevation of privilege vulnerability exists in Microsoft Windows when the MultiPoint management account password is improperly secured. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated privileges.

(CVE-2018-0828)

- A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2018-0840)

- An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. (CVE-2018-0832)

- An information disclosure vulnerability exists when VBScript improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the users computer or data.

(CVE-2018-0847)

- An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2018-0844, CVE-2018-0846)

- A security feature bypass vulnerability exists when Microsoft Edge improperly handles requests of different origins. The vulnerability allows Microsoft Edge to bypass Same-Origin Policy (SOP) restrictions, and to allow requests that should otherwise be ignored. An attacker who successfully exploited the vulnerability could force the browser to send data that would otherwise be restricted. (CVE-2018-0771)

- An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory.

An attacker who successfully exploited the vulnerability could execute code with elevated permissions.

(CVE-2018-0742, CVE-2018-0756, CVE-2018-0820, CVE-2018-0831)

See Also

http://www.nessus.org/u?e2535711

Solution

Apply Cumulative Update KB4074590.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2018-0742
CVE	CVE-2018-0756

CVE	CVE-2018-0757
CVE	CVE-2018-0771
CVE	CVE-2018-0820
CVE	CVE-2018-0821
CVE	CVE-2018-0822
CVE	CVE-2018-0825
CVE	CVE-2018-0826
CVE	CVE-2018-0828
CVE	CVE-2018-0829
CVE	CVE-2018-0830
CVE	CVE-2018-0831
CVE	CVE-2018-0832
CVE	CVE-2018-0834
CVE	CVE-2018-0835
CVE	CVE-2018-0837
CVE	CVE-2018-0838
CVE	CVE-2018-0840
CVE	CVE-2018-0842
CVE	CVE-2018-0844
CVE	CVE-2018-0846
CVE	CVE-2018-0847
CVE	CVE-2018-0857
CVE	CVE-2018-0859
CVE	CVE-2018-0860
CVE	CVE-2018-0861
CVE	CVE-2018-0866
MSKB	4074590
XREF	MSFT:MS18-4074590

Plugin Information:

Published: 2018/02/13, Modified: 2018/03/16

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4074590

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.2068
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4074590

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.2097
```

108289 (2) - KB4088787: Windows 10 Version 1607 and Windows Server 2016 March 2018 Security Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4088787.

It is, therefore, affected by multiple vulnerabilities :

- An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0880, CVE-2018-0882)

- An elevation of privilege vulnerability exists when Storage Services improperly handles objects in memory.

An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2018-0983)

- An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. (CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901, CVE-2018-0904)

- An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs;

view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0816, CVE-2018-0817)

- An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2018-0977)

- A security feature bypass vulnerability exists in Windows Scripting Host which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine.

(CVE-2018-0884)

- An elevation of privilege vulnerability exists in Windows when the Microsoft Video Control mishandles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in system mode. An attacker could then install programs;

view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0881)

- An elevation of privilege vulnerability exists when Internet Explorer fails a check, allowing sandbox escape. An attacker who successfully exploited the vulnerability could use the sandbox escape to elevate privileges on an affected system. This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code

execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted. The update addresses the vulnerability by correcting how Internet Explorer handles zone and integrity settings. (CVE-2018-0942)

- A remote code execution vulnerability exists in the Credential Security Support Provider protocol (CredSSP).

An attacker who successfully exploited this vulnerability could relay user credentials and use them to execute code on the target system. CredSSP is an authentication provider which processes authentication requests for other applications; any application which depends on CredSSP for authentication may be vulnerable to this type of attack. As an example of how an attacker would exploit this vulnerability against Remote Desktop Protocol, the attacker would need to run a specially crafted application and perform a man-in-the-middle attack against a Remote Desktop Protocol session. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting how Credential Security Support Provider protocol (CredSSP) validates requests during the authentication process. To be fully protected against this vulnerability users must enable Group Policy settings on their systems and update their Remote Desktop clients. The Group Policy settings are disabled by default to prevent connectivity problems and users must follow the instructions documented HERE to be fully protected. (CVE-2018-0886)

- An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2018-0891)

- A remote code execution vulnerability exists when Windows Shell does not properly validate file copy destinations. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2018-0883)

- An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the users system. (CVE-2018-0927, CVE-2018-0932)

- A security feature bypass vulnerability exists in the Cryptography Next Generation (CNG) kernel-mode driver (cng.sys) when it fails to properly validate and enforce impersonation levels. An attacker could exploit this vulnerability by convincing a user to run a specially crafted application that is designed to cause CNG to improperly validate impersonation levels, potentially allowing the attacker to gain access to information beyond the access level of the local user. The security update addresses the vulnerability by correcting how the kernel-mode driver validates and enforces impersonation levels. (CVE-2018-0902)

- An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. (CVE-2018-0888)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2018-0876, CVE-2018-0893)

- An information disclosure vulnerability exists when Windows Remote Assistance incorrectly processes XML External Entities (XXE). An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2018-0878)

- An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.

An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2018-0929)

- An elevation of privilege vulnerability exists in Windows when the Desktop Bridge VFS does not take into acccount user/kernel mode when managing file paths. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2018-0877)

- An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior. A locally authenticated attacker could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting the input sanitization error to preclude unintended elevation. (CVE-2018-0868)

- A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash. (CVE-2018-0885)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2018-0889, CVE-2018-0935)

- An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.

(CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0926)

- A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934)

See Also

http://www.nessus.org/u?a4c76068

Solution

Apply Cumulative Update KB4088787.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

BID	103227
BID	103230
BID	103231
BID	103232
BID	103236
BID	103238
BID	103239
BID	103240
BID	103241
BID	103242
BID	103243
BID	103244
BID	103245
BID	103246
BID	103247
BID	103248
BID	103249
BID	103250
BID	103251
BID	103256
BID	103257
BID	103259
BID	103260
BID	103261
BID	103262
BID	103265
BID	103266
BID	103267
BID	103268
BID	103269
BID	103273
BID	103274
BID	103275
BID	103288
BID	103289
BID	103295
BID	103298
BID	103299

BID	103307
BID	103309
BID	103310
BID	103312
BID	103380
BID	103381
CVE	CVE-2018-0811
CVE	CVE-2018-0813
CVE	CVE-2018-0814
CVE	CVE-2018-0816
CVE	CVE-2018-0817
CVE	CVE-2018-0868
CVE	CVE-2018-0872
CVE	CVE-2018-0873
CVE	CVE-2018-0874
CVE	CVE-2018-0876
CVE	CVE-2018-0877
CVE	CVE-2018-0878
CVE	CVE-2018-0880
CVE	CVE-2018-0881
CVE	CVE-2018-0882
CVE	CVE-2018-0883
CVE	CVE-2018-0884
CVE	CVE-2018-0885
CVE	CVE-2018-0886
CVE	CVE-2018-0888
CVE	CVE-2018-0889
CVE	CVE-2018-0891
CVE	CVE-2018-0893
CVE	CVE-2018-0894
CVE	CVE-2018-0895
CVE	CVE-2018-0896
CVE	CVE-2018-0897
CVE	CVE-2018-0898
CVE	CVE-2018-0899
CVE	CVE-2018-0900
CVE	CVE-2018-0901
CVE	CVE-2018-0902
CVE	CVE-2018-0904
CVE	CVE-2018-0926
CVE	CVE-2018-0927
CVE	CVE-2018-0929
CVE	CVE-2018-0931

CVE	CVE-2018-0932
CVE	CVE-2018-0933
CVE	CVE-2018-0934
CVE	CVE-2018-0935
CVE	CVE-2018-0942
CVE	CVE-2018-0977
CVE	CVE-2018-0983
MSKB	4088787
XREF	OSVDB:176606
XREF	OSVDB:176607
XREF	OSVDB:176608
XREF	OSVDB:176610
XREF	OSVDB:176614
XREF	OSVDB:176619
XREF	OSVDB:176621
XREF	OSVDB:176627
XREF	OSVDB:176628
XREF	OSVDB:176629
XREF	OSVDB:176630
XREF	OSVDB:176631
XREF	OSVDB:176632
XREF	OSVDB:176633
XREF	OSVDB:176634
XREF	OSVDB:176635
XREF	OSVDB:176636
XREF	OSVDB:176637
XREF	OSVDB:176638
XREF	OSVDB:176639
XREF	OSVDB:176641
XREF	OSVDB:176642
XREF	OSVDB:176643
XREF	OSVDB:176645
XREF	OSVDB:176646
XREF	OSVDB:176647
XREF	OSVDB:176648
XREF	OSVDB:176649
XREF	OSVDB:176652
XREF	OSVDB:176653
XREF	OSVDB:176654
XREF	OSVDB:176655
XREF	OSVDB:176656
XREF	OSVDB:176659
XREF	OSVDB:176664

XREF	OSVDB:176665
XREF	OSVDB:176667
XREF	OSVDB:176670
XREF	OSVDB:176682
XREF	OSVDB:176683
XREF	OSVDB:176684
XREF	OSVDB:176687
XREF	OSVDB:176688
XREF	OSVDB:176689
XREF	MSFT:MS18-4088787
XREF	IAVA:2018-A-0075
XREF	IAVA:2018-A-0076
XREF	IAVA:2018-A-0080
XREF	IAVA:2018-A-0081

Plugin Information:

Published: 2018/03/13, Modified: 2018/03/22

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4088787

C:\Windows\system32\win32kfull.sys has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.2125
```

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4088787

C:\Windows\system32\win32kfull.sys has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.2155
```

87253 (1) - MS15-124: Cumulative Security Update for Internet Explorer (3116180)

Synopsis

The remote host has a web browser installed that is affected by multiple vulnerabilities.

Description

The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. It is, therefore, affected by multiple vulnerabilities, the majority of which are remote code execution vulnerabilities. An unauthenticated, remote attacker can exploit these issues by convincing a user to visit a specially crafted website, resulting in the execution of arbitrary code in the context of the current user.

See Also

https://technet.microsoft.com/library/security/MS15-124

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	78481
BID	78482
BID	78483
BID	78484
BID	78485
BID	78486
BID	78487
BID	78488
BID	78489
BID	78490
BID	78491

BID	78492
BID	78494
BID	78495
BID	78507
BID	78508
BID	78526
BID	78527
BID	78528
BID	78529
BID	78530
BID	78531
BID	78532
BID	78533
BID	78534
BID	78535
BID	78536
BID	78537
BID	78538
BID	78540
CVE	CVE-2015-6083
CVE	CVE-2015-6134
CVE	CVE-2015-6135
CVE	CVE-2015-6136
CVE	CVE-2015-6138
CVE	CVE-2015-6139
CVE	CVE-2015-6140
CVE	CVE-2015-6141
CVE	CVE-2015-6142
CVE	CVE-2015-6143
CVE	CVE-2015-6144
CVE	CVE-2015-6145
CVE	CVE-2015-6146
CVE	CVE-2015-6147
CVE	CVE-2015-6148
CVE	CVE-2015-6149
CVE	CVE-2015-6150
CVE	CVE-2015-6151
CVE	CVE-2015-6152
CVE	CVE-2015-6153
CVE	CVE-2015-6154
CVE	CVE-2015-6155
CVE	CVE-2015-6156
CVE	CVE-2015-6157

CVE	CVE-2015-6158
CVE	CVE-2015-6159
CVE	CVE-2015-6160
CVE	CVE-2015-6161
CVE	CVE-2015-6162
CVE	CVE-2015-6164
MSKB	3104002
MSKB	3116869
MSKB	3116900
MSKB	3125869
XREF	OSVDB:131290
XREF	OSVDB:131291
XREF	OSVDB:131292
XREF	OSVDB:131293
XREF	OSVDB:131294
XREF	OSVDB:131295
XREF	OSVDB:131296
XREF	OSVDB:131297
XREF	OSVDB:131298
XREF	OSVDB:131299
XREF	OSVDB:131300
XREF	OSVDB:131301
XREF	OSVDB:131302
XREF	OSVDB:131303
XREF	OSVDB:131304
XREF	OSVDB:131305
XREF	OSVDB:131306
XREF	OSVDB:131307
XREF	OSVDB:131308
XREF	OSVDB:131309
XREF	OSVDB:131310
XREF	OSVDB:131311
XREF	OSVDB:131312
XREF	OSVDB:131313
XREF	OSVDB:131314
XREF	OSVDB:131315
XREF	OSVDB:131316
XREF	OSVDB:131317
XREF	OSVDB:131318
XREF	OSVDB:131319
XREF	MSFT:MS15-124

Plugin Information:

Published: 2015/12/08, Modified: 2017/07/24

Plugin Output

192.168.1.2 (tcp/445)

```
ASLR hardening settings for Internet Explorer in KB3125869
have not been applied. The following DWORD keys must be
created with a value of 1:
  - HKLM\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl
\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl
\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe
```

99365 (1) - Security and Quality Rollup for .NET Framework (April 2017)

Synopsis

The remote Windows host has a software framework installed that is affected by an arbitrary code execution vulnerability.

Description

The version of Microsoft .NET Framework installed on the remote Windows host is missing a security update. It is, therefore, affected by an arbitrary code execution vulnerability due to a failure to properly validate input before loading libraries. A local attacker can exploit this to execute arbitrary code with elevated privileges.

See Also

http://www.nessus.org/u?af87bdc8

http://www.nessus.org/u?75fb2a89

Solution

Microsoft has released a set of patches for Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:ND)

STIG Severity

II

References

BID	97447
CVE	CVE-2017-0160
MSKB	4014545

MSKB	4014546
MSKB	4014547
MSKB	4014548
MSKB	4014549
MSKB	4014550
MSKB	4014551
MSKB	4014552
MSKB	4014553
MSKB	4014555
MSKB	4014556
MSKB	4014557
MSKB	4014558
MSKB	4014559
MSKB	4014560
MSKB	4014561
MSKB	4014562
MSKB	4014563
MSKB	4014564
MSKB	4014565
MSKB	4014566
MSKB	4014567
MSKB	4014571
MSKB	4014572
MSKB	4014573
MSKB	4014574
MSKB	4015217
MSKB	4015219
MSKB	4015221
MSKB	4015583
XREF	OSVDB:155341
XREF	IAVB:2017-B-0045
XREF	MSFT:MS17-4014545
XREF	MSFT:MS17-4014546
XREF	MSFT:MS17-4014547
XREF	MSFT:MS17-4014548
XREF	MSFT:MS17-4014549
XREF	MSFT:MS17-4014550
XREF	MSFT:MS17-4014551
XREF	MSFT:MS17-4014552
XREF	MSFT:MS17-4014553
XREF	MSFT:MS17-4014555
XREF	MSFT:MS17-4014556
XREF	MSFT:MS17-4014557

XREF	MSFT:MS17-4014558
XREF	MSFT:MS17-4014559
XREF	MSFT:MS17-4014560
XREF	MSFT:MS17-4014561
XREF	MSFT:MS17-4014562
XREF	MSFT:MS17-4014563
XREF	MSFT:MS17-4014564
XREF	MSFT:MS17-4014565
XREF	MSFT:MS17-4014566
XREF	MSFT:MS17-4014567
XREF	MSFT:MS17-4014571
XREF	MSFT:MS17-4014572
XREF	MSFT:MS17-4014573
XREF	MSFT:MS17-4014574
XREF	MSFT:MS17-4015217
XREF	MSFT:MS17-4015219
XREF	MSFT:MS17-4015221
XREF	MSFT:MS17-4015583

Plugin Information:

Published: 2017/04/14, Modified: 2018/01/30

Plugin Output

192.168.1.2 (tcp/445)

```
Microsoft .NET Framework 3.5
The remote host is missing one of the following rollup KBs :
  - 4015217

C:\Windows\Microsoft.NET\Framework\v2.0.50727\Wminet_utils.dll has not been patched.
    Remote version : 2.0.50727.8745
    Should be      : 2.0.50727.8758
```

102262 (1) - Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 26.0.0.137. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists due to an unspecified flaw. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to disclose sensitive information. (CVE-2017-3085)

- A remote code execution vulnerability exists due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to execute arbitrary code. (CVE-2017-3106)

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-23.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 26.0.0.151 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	100191
CVE	CVE-2017-3085
CVE	CVE-2017-3106
XREF	OSVDB:162718
XREF	OSVDB:162719

Plugin Information:

Published: 2017/08/08, Modified: 2017/09/14

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 26.0.0.151
```

102266 (1) - KB4034662: Security update for Adobe Flash Player (August 2017)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4034662. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists due to an unspecified flaw. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to disclose sensitive information. (CVE-2017-3085)

- A remote code execution vulnerability exists due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to execute arbitrary code. (CVE-2017-3106)

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-23.html

http://www.nessus.org/u?a5a1122e

http://www.nessus.org/u?a8fb45ae

Solution

Microsoft has released a set of patches for Windows 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	100191
CVE	CVE-2017-3085
CVE	CVE-2017-3106
MSKB	4034662
XREF	OSVDB:162718
XREF	OSVDB:162719
XREF	MSFT:MS17-4034662

Plugin Information:

Published: 2017/08/08, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 26.0.0.151

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

102993 (1) - Google Chrome < 61.0.3163.79 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 61.0.3163.79. It is, therefore, affected by the following vulnerabilities :

- A use-after-free error exists in PDFium. A unauthenticated, remote attacker can exploit this to execute arbitrary code.

(CVE-2017-5111)

- A heap buffer overflow condition exists in WebGL that allows an unauthenticated, remote attacker to execute arbitrary code.

(CVE-2017-5112)

- A heap buffer overflow condition exists in Skia that allows an unauthenticated, remote attacker to execute arbitrary code.

(CVE-2017-5113)

- An unspecified memory lifecycle issue exists in PDFium that allow an unauthenticated, remote attacker to have an unspecified impact (CVE-2017-5114)

- An unspecified type confusion errors exist in V8.

(CVE-2017-5115, CVE-2017-5116)

- An unspecified uninitialized value flaws exist in Skia that allows an unauthenticated, remote attacker to have an unspecified impact.

(CVE-2017-5117, CVE-2017-5119)

- An unspecified security bypass vulnerability exists in Blink. An unauthenticated, remote attacker can exploit this to bypass content security policy. (CVE-2017-5118)

- An unspecified flaw allows HTTPS downgrade during redirection.

(CVE-2017-5120)

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?67b28931

Solution

Upgrade to Google Chrome version 61.0.3163.79 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	100610
CVE	CVE-2017-5111
CVE	CVE-2017-5112
CVE	CVE-2017-5113
CVE	CVE-2017-5114
CVE	CVE-2017-5115
CVE	CVE-2017-5116
CVE	CVE-2017-5117
CVE	CVE-2017-5118
CVE	CVE-2017-5119
CVE	CVE-2017-5120
XREF	OSVDB:164716
XREF	OSVDB:164694
XREF	OSVDB:164695
XREF	OSVDB:164696
XREF	OSVDB:164697
XREF	OSVDB:164698
XREF	OSVDB:164699
XREF	OSVDB:164700
XREF	OSVDB:164701
XREF	OSVDB:164702
XREF	OSVDB:164703
XREF	OSVDB:164704
XREF	OSVDB:164705

XREF	OSVDB:164706
XREF	OSVDB:164707
XREF	OSVDB:164708
XREF	OSVDB:164709
XREF	OSVDB:164710
XREF	OSVDB:164711
XREF	OSVDB:164712
XREF	OSVDB:164713
XREF	OSVDB:164714

Plugin Information:

Published: 2017/09/07, Modified: 2018/01/22

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 61.0.3163.79
```

103122 (1) - Security Updates for Microsoft Publisher Products (September 2017)

Synopsis

The Microsoft Publisher Products are missing a security update.

Description

The Microsoft Publisher Products are missing a security update. It is, therefore, affected by the following vulnerability :

- A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory.

(CVE-2017-8725)

See Also

http://www.nessus.org/u?7cd17670

http://www.nessus.org/u?a1417166

Solution

Microsoft has released the following security updates to address this issue:

-KB3114428

-KB3141537

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	100758
CVE	CVE-2017-8725
MSKB	3114428
MSKB	3141537
XREF	OSVDB:165254
XREF	MSFT:MS17-3114428
XREF	MSFT:MS17-3141537
XREF	IAVA:2017-A-0274

Plugin Information:

Published: 2017/09/12, Modified: 2017/09/14

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Publisher 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Mspub.exe has not been patched.
  Remote version    : 14.0.7162.5000
  Fixed version     : 14.0.7188.5000
```

103124 (1) - Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 26.0.0.151. It is, therefore, affected by multiple vulnerabilities :

- An unspecified memory corruption flaw exists that is caused by input not being properly validated. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to to corrupt memory and potentially execute arbitrary code.

(CVE-2017-11281, CVE-2017-11282)

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-28.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 27.0.0.130 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	100710

BID	100716
CVE	CVE-2017-11281
CVE	CVE-2017-11282
XREF	OSVDB:165215
XREF	OSVDB:165216

Plugin Information:

Published: 2017/09/12, Modified: 2017/11/13

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 27.0.0.130
```

103133 (1) - Security Updates for Microsoft Office Products (September 2017)

Synopsis

The Microsoft Office Products are affected by multiple vulnerabilities.

Description

The Microsoft Office Products are missing security updates.

It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory.

(CVE-2017-8630, CVE-2017-8744)

- A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit this vulnerability. In a web- based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. The security update addresses the vulnerabilities by correcting how the Windows font library handles embedded fonts. (CVE-2017-8682)

- An information disclosure vulnerability exists when Windows Uniscribe improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document or by convincing a user to visit an untrusted webpage.

The update addresses the vulnerability by correcting how Windows Uniscribe handles objects in memory.

(CVE-2017-8695)

- A remote code execution vulnerability exists due to the way Windows Uniscribe handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit this vulnerability: In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit this

vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content.

Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document file.The security update addresses the vulnerability by correcting how Windows Uniscribe handles objects in memory. (CVE-2017-8696)

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website.

Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory.

(CVE-2017-8742)

- An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. Note that where the severity is indicated as Critical in the Affected Products table, the Preview Pane is an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how GDI handles memory addresses. (CVE-2017-8676)

See Also

http://www.nessus.org/u?8d24309b

http://www.nessus.org/u?c95ea355

http://www.nessus.org/u?69c44d41

http://www.nessus.org/u?40a27f00

http://www.nessus.org/u?a714c54e

http://www.nessus.org/u?b84ca703

http://www.nessus.org/u?607de17a

http://www.nessus.org/u?f846aeb6

http://www.nessus.org/u?7601f27e

http://www.nessus.org/u?4928d07a

http://www.nessus.org/u?fa6bb9d8

http://www.nessus.org/u?7d1e5263

http://www.nessus.org/u?b27cd572

http://www.nessus.org/u?7194ec3f

http://www.nessus.org/u?9ecdeba5

http://www.nessus.org/u?b2751aff

Solution

Microsoft has released security updates for Microsoft Office Products.

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:ND)

STIG Severity

II

References

BID	100732
BID	100741
BID	100748
BID	100755
BID	100772
BID	100773
BID	100780
CVE	CVE-2017-8630
CVE	CVE-2017-8676
CVE	CVE-2017-8682
CVE	CVE-2017-8695
CVE	CVE-2017-8696
CVE	CVE-2017-8742
CVE	CVE-2017-8744
MSKB	4011055

MSKB	3213649
MSKB	4011038
MSKB	3213626
MSKB	3213646
MSKB	3213641
MSKB	3213642
MSKB	3213564
MSKB	3203474
MSKB	3213638
MSKB	4011103
MSKB	4011126
MSKB	4011063
MSKB	4011062
MSKB	3213551
MSKB	3213631
XREF	OSVDB:165239
XREF	OSVDB:165241
XREF	OSVDB:165271
XREF	OSVDB:165272
XREF	OSVDB:165280
XREF	OSVDB:165286
XREF	OSVDB:165294
XREF	MSFT:MS17-4011055
XREF	MSFT:MS17-3213649
XREF	MSFT:MS17-4011038
XREF	MSFT:MS17-3213626
XREF	MSFT:MS17-3213646
XREF	MSFT:MS17-3213641
XREF	MSFT:MS17-3213642
XREF	MSFT:MS17-3213564
XREF	MSFT:MS17-3203474
XREF	MSFT:MS17-3213638
XREF	MSFT:MS17-4011103
XREF	MSFT:MS17-4011126
XREF	MSFT:MS17-4011063
XREF	MSFT:MS17-4011062
XREF	MSFT:MS17-3213551
XREF	MSFT:MS17-3213631
XREF	IAVA:2017-A-0274

Plugin Information:

Published: 2017/09/12, Modified: 2017/09/22

Plugin Output

192.168.1.2 (tcp/445)

```
Product : Microsoft Office 2010 SP2
KB      : 4011055
- C:\Program Files (x86)\Common Files\Microsoft Shared\Office14\mso.dll has not been patched.
  Remote version : 14.0.7184.5000
  Should be      : 14.0.7188.5002

Product : Microsoft Office 2010 SP2
KB      : 3213626
- C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\Wpft632.cnv has not been patched.
  Remote version : 2010.1400.7151.5000
  Should be      : 2010.1400.7188.5000
```

103136 (1) - Security Updates for Microsoft Powerpoint Products (September 2017)

Synopsis

The Microsoft Powerpoint Products are affected by multiple vulnerabilities.

Description

The Microsoft Powerpoint Products are missing security updates. It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website.

Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory.

(CVE-2017-8742, CVE-2017-8743)

See Also

http://www.nessus.org/u?acec2355

http://www.nessus.org/u?8d9bf308

http://www.nessus.org/u?7e2fc194

Solution

Microsoft has released the following security updates to address this issue:

-KB4011041

-KB3128027

-KB4011069

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	100741
BID	100746
CVE	CVE-2017-8742
CVE	CVE-2017-8743
MSKB	3213642
MSKB	4011041
MSKB	3128027
MSKB	4011069
XREF	OSVDB:165240
XREF	OSVDB:165241
XREF	MSFT:MS17-3213642
XREF	MSFT:MS17-4011041
XREF	MSFT:MS17-3128027
XREF	MSFT:MS17-4011069
XREF	IAVA:2017-A-0274

Plugin Information:

Published: 2017/09/12, Modified: 2017/09/14

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : PowerPoint 2010
- C:\Program Files (x86)\Microsoft Office\Office14\ppcore.dll has not been patched.
```

```
  Remote version    : 14.0.7176.5000
  Fixed version     : 14.0.7188.5000
```

103137 (1) - Security and Quality Rollup for .NET Framework (Sep 2017)

Synopsis

The remote Windows host has a software framework installed that is affected by a security feature bypass vulnerability.

Description

The .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by the following vulnerability:

- A remote code execution vulnerability exists when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploited this vulnerability in software using the .NET framework could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

(CVE-2017-8759)

See Also

http://www.nessus.org/u?39028b0b

http://www.nessus.org/u?a9b7377f

Solution

Microsoft has released a set of patches for Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

9.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:C)

CVSS Temporal Score

8.2 (CVSS2#E:H/RL:OF/RC:ND)

STIG Severity

I

References

BID	100742
CVE	CVE-2017-8759
MSKB	4041086
MSKB	4041093
MSKB	4041083
MSKB	4041090
MSKB	4041084
MSKB	4041091
MSKB	4041085
MSKB	4041092
MSKB	4038781
MSKB	4038783
MSKB	4038782
MSKB	4038788
XREF	OSVDB:165223
XREF	MSFT:MS17-4041086
XREF	MSFT:MS17-4041093
XREF	MSFT:MS17-4041083
XREF	MSFT:MS17-4041090
XREF	MSFT:MS17-4041084
XREF	MSFT:MS17-4041091
XREF	MSFT:MS17-4041085
XREF	MSFT:MS17-4041092
XREF	MSFT:MS17-4038781
XREF	MSFT:MS17-4038783
XREF	MSFT:MS17-4038782
XREF	MSFT:MS17-4038788
XREF	IAVA:2017-A-0272

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information:

Published: 2017/09/12, Modified: 2018/03/02

Plugin Output

192.168.1.2 (tcp/445)

```
Microsoft .NET Framework 4.7
The remote host is missing one of the following rollup KBs :
```

```
  - 4038782

C:\Windows\Microsoft.NET\Framework\v4.0.30319\system.runtime.remoting.dll has not been patched.
    Remote version : 4.7.2053.0
    Should be      : 4.7.2114.0

Microsoft .NET Framework 3.5
The remote host is missing one of the following rollup KBs :
  - 4038782

C:\Windows\Microsoft.NET\Framework\v2.0.50727\system.runtime.remoting.dll has not been patched.
    Remote version : 2.0.50727.8745
    Should be      : 2.0.50727.8771
```

103220 (1) - KB4038806: Security update for Adobe Flash Player (September 2017)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4038806. It is, therefore, affected by multiple remote code execution vulnerabilies in Adobe Flash Player.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-28.html

http://www.nessus.org/u?65af4a4d

http://www.nessus.org/u?bca86c2c

Solution

Microsoft has released a set of patches for Windows 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	100710
BID	100716
CVE	CVE-2017-11281
CVE	CVE-2017-11282

MSKB	4038806
XREF	OSVDB:165215
XREF	OSVDB:165216
XREF	MSFT:MS17-4038806

Plugin Information:

Published: 2017/09/14, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 27.0.0.130

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

103421 (1) - Google Chrome < 61.0.3163.100 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 61.0.3163.100. It is, therefore, affected by two out-of- bounds access flaws related to the V8 JavaScript engine that have unspecified impact.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?39b75732

Solution

Upgrade to Google Chrome version 61.0.3163.100 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	100947
CVE	CVE-2017-5121
CVE	CVE-2017-5122
XREF	OSVDB:165923

Plugin Information:

Published: 2017/09/22, Modified: 2017/10/26

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 61.0.3163.100
```

103752 (1) - Security Updates for Outlook (October 2017)

Synopsis

The version of Outlook installed on the remote host is affected by multiple vulnerabilities.

Description

The version of Microsoft Outlook installed on the remote host is missing security updates. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists when Microsoft Outlook fails to establish a secure connection. An attacker who exploited the vulnerability could use it to obtain the email content of a user. The security update addresses the vulnerability by preventing Outlook from disclosing user email content.

(CVE-2017-11776)

- A security feature bypass vulnerability exists when Microsoft Office improperly handles objects in memory.

An attacker who successfully exploited the vulnerability could execute arbitrary commands. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability, and then convince users to open the document file and interact with the document. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. (CVE-2017-11774)

See Also

http://www.nessus.org/u?67eda8b2

http://www.nessus.org/u?a6c94157

http://www.nessus.org/u?fcfcd1f7

Solution

Microsoft has released a set of patches for Outlook 2010, 2013, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	101098
BID	101106
CVE	CVE-2017-11774
CVE	CVE-2017-11776
MSKB	4011162
MSKB	4011178
MSKB	4011196
XREF	OSVDB:167092
XREF	OSVDB:167094
XREF	MSFT:MS17-4011162
XREF	MSFT:MS17-4011178
XREF	MSFT:MS17-4011196
XREF	IAVA:2017-A-0291

Plugin Information:

Published: 2017/10/10, Modified: 2017/10/12

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Outlook 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Outlook.exe has not been patched.
  Remote version    : 14.0.7187.5000
  Fixed version     : 14.0.7189.5000
```

103784 (1) - Security Updates for Microsoft Office Products (October 2017)

Synopsis

The Microsoft Office Products are affected by multiple vulnerabilities.

Description

The Microsoft Office Products are missing security updates.

It is, therefore, affected by multiple vulnerabilities :

- Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure.

- A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. (CVE-2017-11825)

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2017-11826)

See Also

http://www.nessus.org/u?a8a017c7

http://www.nessus.org/u?6c08bcd5

http://www.nessus.org/u?c4720201

http://www.nessus.org/u?e43bd8f6

http://www.nessus.org/u?3fd7628b

http://www.nessus.org/u?3c605abc

https://technet.microsoft.com/en-us/office/mt465751

http://www.nessus.org/u?544bebd5

http://www.nessus.org/u?005e6964

http://www.nessus.org/u?5d96e89f

http://www.nessus.org/u?4e757244

http://www.nessus.org/u?5e7317f0

Solution

Microsoft has released security updates for Microsoft Office Products.

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

II

References

BID	101124
BID	101219
CVE	CVE-2017-11825
CVE	CVE-2017-11826
MSKB	3172524
MSKB	3172531
MSKB	4011185
MSKB	2920723
MSKB	2553338
MSKB	2837599
MSKB	4011222
MSKB	3213648
MSKB	4011232
MSKB	3213630
MSKB	3213627
XREF	OSVDB:167045
XREF	OSVDB:167046
XREF	MSFT:MS17-3172524
XREF	MSFT:MS17-3172531
XREF	MSFT:MS17-4011185
XREF	MSFT:MS17-2920723
XREF	MSFT:MS17-2553338
XREF	MSFT:MS17-2837599
XREF	MSFT:MS17-4011222
XREF	MSFT:MS17-3213648
XREF	MSFT:MS17-4011232

XREF	MSFT:MS17-32136304
XREF	MSFT:MS17-3213627
XREF	IAVA:2017-A-0291

Exploitable With

Core Impact (true)

Plugin Information:

Published: 2017/10/11, Modified: 2017/11/03

Plugin Output

192.168.1.2 (tcp/445)

```
  Product : Microsoft Office 2010 SP2
  KB      : 2553338
  - C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\ose.exe has not been patched.
    Remote version : 14.0.4730.1010
    Should be      : 14.0.7189.5000

  Product : Microsoft Office 2010 SP2
  KB      : 2837599
  - C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\Office Setup Controller\osetup.dll
has not been patched.
    Remote version : 14.0.7106.5000
    Should be      : 14.0.7189.5000

  Product           : Word 2010
  - C:\Program Files (x86)\Microsoft Office\Office14\WinWord.exe has not been patched.
    Remote version    : 14.0.7182.5000
    Fixed version     : 14.0.7189.5001
```

103876 (1) - Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.

(CVE-2017-11780)

- A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server. An attacker who exploited this vulnerability could cause the affected system to crash. To attempt to exploit this issue, an attacker would need to send specially crafted SMB requests to the target system. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests. The security update addresses the vulnerability by correcting the manner in which SMB handles specially crafted client requests.

(CVE-2017-11781)

Note that Microsoft uses AC:H for these two vulnerabilities. This could mean that an exploitable target is configured in a certain way that may include that a publicly accessible file share is available and share enumeration is allowed for anonymous users.

See Also

http://www.nessus.org/u?72a4ce73

http://www.nessus.org/u?42adf289

Solution

Microsoft has released a set of patches for Windows 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.6 (CVSS2#E:U/RL:OF/RC:C)

References

BID	101110
BID	101140
CVE	CVE-2017-11780
CVE	CVE-2017-11781
MSKB	4041676
MSKB	4041678
MSKB	4041679
MSKB	4041681
MSKB	4041687
MSKB	4041689
MSKB	4041690
MSKB	4041691
MSKB	4041693
MSKB	4041995
MSKB	4042895
XREF	OSVDB:167088
XREF	OSVDB:167089
XREF	MSFT:MS17-4041676
XREF	MSFT:MS17-4041678
XREF	MSFT:MS17-4041679
XREF	MSFT:MS17-4041681
XREF	MSFT:MS17-4041687
XREF	MSFT:MS17-4041689
XREF	MSFT:MS17-4041690
XREF	MSFT:MS17-4041691
XREF	MSFT:MS17-4041693
XREF	MSFT:MS17-4041995
XREF	MSFT:MS17-4042895

Plugin Information:

Published: 2017/10/17, Modified: 2017/10/18

Plugin Output

192.168.1.2 (tcp/445)

103922 (1) - Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)

Synopsis

The remote Windows host has a browser plugin installed that is affected by a type confusion vulnerability.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 27.0.0.159. It is, therefore, affected by an unspecified type confusion flaw that is caused by input not being properly validated. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to trigger the vulnerability and potentially execute arbitrary code.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-32.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 27.0.0.170 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.1 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	101286
CVE	CVE-2017-11292
XREF	OSVDB:167361

Plugin Information:

Published: 2017/10/18, Modified: 2017/11/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 27.0.0.170
```

103924 (1) - KB4049179: Security update for Adobe Flash Player (October 2017)

Synopsis

The remote Windows host has a browser plugin installed that is affected by a type confusion vulnerability.

Description

The remote Windows host is missing security update KB4049179. It is, therefore, affected by an unspecified type confusion flaw that is caused by input not being properly validated. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a website containing specially crafted Flash content, to trigger the vulnerability and potentially execute arbitrary code.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-32.html

http://www.nessus.org/u?6b756c8b

http://www.nessus.org/u?ecb4c411

Solution

Microsoft has released a set of patches for Windows 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.1 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	101286
CVE	CVE-2017-11292

MSKB	4049179
XREF	OSVDB:167361
XREF	MSFT:MS17-4049179

Plugin Information:

Published: 2017/10/18, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 27.0.0.170

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

103933 (1) - Google Chrome < 62.0.3202.62 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 62.0.3202.62. It is, therefore, affected by multiple vulnerabilities as noted in Chrome stable channel update release notes.

Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?441fea3d

Solution

Upgrade to Google Chrome version 62.0.3202.62 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-5124
CVE	CVE-2017-5125
CVE	CVE-2017-5126

CVE	CVE-2017-5127
CVE	CVE-2017-5128
CVE	CVE-2017-5129
CVE	CVE-2017-5132
CVE	CVE-2017-5130
CVE	CVE-2017-5131
CVE	CVE-2017-5133
CVE	CVE-2017-15386
CVE	CVE-2017-15387
CVE	CVE-2017-15388
CVE	CVE-2017-15389
CVE	CVE-2017-15390
CVE	CVE-2017-15391
CVE	CVE-2017-15392
CVE	CVE-2017-15393
CVE	CVE-2017-15394
CVE	CVE-2017-15395
XREF	OSVDB:167636
XREF	OSVDB:167637
XREF	OSVDB:167638
XREF	OSVDB:167649
XREF	OSVDB:167652
XREF	OSVDB:167653
XREF	OSVDB:167654
XREF	OSVDB:167655
XREF	OSVDB:167656
XREF	OSVDB:167657
XREF	OSVDB:167658
XREF	OSVDB:167659
XREF	OSVDB:167660
XREF	OSVDB:167661
XREF	OSVDB:167662
XREF	OSVDB:167663
XREF	OSVDB:167664
XREF	OSVDB:167665
XREF	OSVDB:167666
XREF	OSVDB:167667
XREF	OSVDB:167668
XREF	OSVDB:167669
XREF	OSVDB:167670
XREF	OSVDB:167671
XREF	OSVDB:167672
XREF	OSVDB:167676

XREF OSVDB:167679

Plugin Information:

Published: 2017/10/18, Modified: 2017/12/01

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 62.0.3202.62
```

104434 (1) - Google Chrome < 62.0.3202.89 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 62.0.3202.89. It is, therefore, affected by multiple vulnerabilities as noted in Chrome stable channel update release notes.

Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?4af6a216

Solution

Upgrade to Google Chrome version 62.0.3202.89 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-15398
CVE	CVE-2017-15399
XREF	OSVDB:168678

XREF OSVDB:168679
XREF OSVDB:168696

Plugin Information:

Published: 2017/11/07, Modified: 2017/12/18

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 62.0.3202.89
```

104544 (1) - Adobe Flash Player <= 27.0.0.183 (APSB17-33)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 27.0.0.183. It is therefore affected by multiple remote code execution vulnerabilities.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-33.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 27.0.0.187 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	101837
CVE	CVE-2017-11213
CVE	CVE-2017-11215
CVE	CVE-2017-11225
CVE	CVE-2017-3112
CVE	CVE-2017-3114
XREF	OSVDB:169124
XREF	OSVDB:169125
XREF	OSVDB:169126

XREF OSVDB:169127
XREF OSVDB:169128

Plugin Information:

Published: 2017/11/14, Modified: 2017/12/18

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 27.0.0.187
```

104547 (1) - KB4048951: Security update for Adobe Flash Player (November 2017)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4048951. It is, therefore, affected by multiple remote code execution vulnerabilities in Adobe Flash Player.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-33.html

http://www.nessus.org/u?0a5b9bb5

Solution

Microsoft has released KB4048951 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	101837
CVE	CVE-2017-11213
CVE	CVE-2017-11215
CVE	CVE-2017-11225
CVE	CVE-2017-3112
CVE	CVE-2017-3114
MSKB	4048951
XREF	OSVDB:169124
XREF	OSVDB:169125

XREF	OSVDB:169126
XREF	OSVDB:169127
XREF	OSVDB:169128
XREF	MSFT:MS17-4048951

Plugin Information:

Published: 2017/11/14, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 27.0.0.187

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

104557 (1) - Security Updates for Microsoft Office Products (November 2017)

Synopsis

The Microsoft Office Products are affected by multiple vulnerabilities.

Description

The Microsoft Office Products are missing security updates.

It is, therefore, affected by multiple vulnerabilities :

- Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure.

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2017-11854)

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2017-11882)

See Also

http://www.nessus.org/u?0f1b55d1

http://www.nessus.org/u?7c504489

http://www.nessus.org/u?df348bb4

http://www.nessus.org/u?4a238ff7

http://www.nessus.org/u?b3ad665b

http://www.nessus.org/u?ddf439cf

http://www.nessus.org/u?1df91bdd

http://www.nessus.org/u?5199de26

Solution

Microsoft has released security updates for Microsoft Office Products.

Risk Factor

High

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:ND)

STIG Severity

II

References

BID	101746
BID	101757
CVE	CVE-2017-11854
CVE	CVE-2017-11882
MSKB	3162047
MSKB	4011268
MSKB	4011604
MSKB	4011262
MSKB	4011618
XREF	OSVDB:169235
XREF	OSVDB:169255
XREF	MSFT:MS17-3162047
XREF	MSFT:MS17-4011268
XREF	MSFT:MS17-4011604
XREF	MSFT:MS17-4011262
XREF	MSFT:MS17-4011618
XREF	IAVA:2017-A-0337

Exploitable With

Core Impact (true)

Plugin Information:

Published: 2017/11/14

Plugin Output

192.168.1.2 (tcp/445)

```
Product : Microsoft Office 2010 SP2
KB      : 4011618
- C:\Program Files (x86)\Common Files\Microsoft Shared\Equation\eqnedt32.exe has not been patched.
  Remote version : 2000.11.9.0
  Should be      : 2017.8.14.0
```

105152 (1) - Google Chrome < 63.0.3239.84 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 63.0.3239.84. It is, therefore, affected by multiple vulnerabilities as noted in Chrome stable channel update release notes for Wednesday, December 6, 2017. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?98a7b4bd

Solution

Upgrade to Google Chrome version 63.0.3239.84 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-15407
CVE	CVE-2017-15408
CVE	CVE-2017-15409

CVE	CVE-2017-15410
CVE	CVE-2017-15411
CVE	CVE-2017-15412
CVE	CVE-2017-15413
CVE	CVE-2017-15414
CVE	CVE-2017-15415
CVE	CVE-2017-15416
CVE	CVE-2017-15417
CVE	CVE-2017-15418
CVE	CVE-2017-15419
CVE	CVE-2017-15420
CVE	CVE-2017-15422
CVE	CVE-2017-15423
CVE	CVE-2017-15424
CVE	CVE-2017-15425
CVE	CVE-2017-15426
CVE	CVE-2017-15427
XREF	OSVDB:170316
XREF	OSVDB:170317
XREF	OSVDB:170318
XREF	OSVDB:170405
XREF	OSVDB:170406
XREF	OSVDB:170407
XREF	OSVDB:170408
XREF	OSVDB:170409
XREF	OSVDB:170409
XREF	OSVDB:170410
XREF	OSVDB:170411
XREF	OSVDB:170412
XREF	OSVDB:170413
XREF	OSVDB:170414
XREF	OSVDB:170415
XREF	OSVDB:170416
XREF	OSVDB:170417
XREF	OSVDB:170418
XREF	OSVDB:170419
XREF	OSVDB:170420
XREF	OSVDB:170421
XREF	OSVDB:170422
XREF	OSVDB:170437
XREF	OSVDB:170454
XREF	OSVDB:170455
XREF	OSVDB:170456

XREF	OSVDB:170457
XREF	OSVDB:170458
XREF	OSVDB:170459
XREF	OSVDB:170460
XREF	OSVDB:170461
XREF	OSVDB:170462
XREF	OSVDB:170463
XREF	OSVDB:170464
XREF	OSVDB:170465
XREF	OSVDB:170466
XREF	OSVDB:170467
XREF	OSVDB:170468

Plugin Information:

Published: 2017/12/11, Modified: 2018/01/04

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 63.0.3239.84
```

105180 (1) - KB4053579: Windows 10 Version 1607 and Windows Server 2016 December 2017 Security Update

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4053579.

It is, therefore, affected by multiple vulnerabilities :

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11889, CVE-2017-11893, CVE-2017-11905, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11914, CVE-2017-11918)

- A security feature bypass exists when Device Guard incorrectly validates an untrusted file. An attacker who successfully exploited this vulnerability could make an unsigned file appear to be signed. Because Device Guard relies on the signature to determine the file is non- malicious, Device Guard could then allow a malicious file to execute. In an attack scenario, an attacker could make an untrusted file appear to be a trusted file. The update addresses the vulnerability by correcting how Device Guard handles untrusted files.

(CVE-2017-11899)

- An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system.

(CVE-2017-11919)

- A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11888)

- A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-11886, CVE-2017-11890, CVE-2017-11901, CVE-2017-11903, CVE-2017-11907, CVE-2017-11913)

- A remote code execution vulnerability exists in RPC if the server has Routing and Remote Access enabled. An attacker who successfully exploited this vulnerability could execute code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2017-11885)

- A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2017-11894, CVE-2017-11895, CVE-2017-11912, CVE-2017-11930)

- An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.

An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2017-11887, CVE-2017-11906)

- An information disclosure vulnerability exists when the Windows its:// protocol handler unnecessarily sends traffic to a remote site in order to determine the zone of a provided URL. This could potentially result in the disclosure of sensitive information to a malicious site.

(CVE-2017-11927)

See Also

http://www.nessus.org/u?d6fee547

Solution

Apply security update KB4053579.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	102045
BID	102046
BID	102047
BID	102050
BID	102053
BID	102054
BID	102055
BID	102058
BID	102062

BID	102063
BID	102065
BID	102077
BID	102078
BID	102080
BID	102081
BID	102082
BID	102085
BID	102086
BID	102087
BID	102088
BID	102089
BID	102091
BID	102092
BID	102093
BID	102095
CVE	CVE-2017-11885
CVE	CVE-2017-11886
CVE	CVE-2017-11887
CVE	CVE-2017-11888
CVE	CVE-2017-11889
CVE	CVE-2017-11890
CVE	CVE-2017-11893
CVE	CVE-2017-11894
CVE	CVE-2017-11895
CVE	CVE-2017-11899
CVE	CVE-2017-11901
CVE	CVE-2017-11903
CVE	CVE-2017-11905
CVE	CVE-2017-11906
CVE	CVE-2017-11907
CVE	CVE-2017-11909
CVE	CVE-2017-11910
CVE	CVE-2017-11911
CVE	CVE-2017-11912
CVE	CVE-2017-11913
CVE	CVE-2017-11914
CVE	CVE-2017-11918
CVE	CVE-2017-11919
CVE	CVE-2017-11927
CVE	CVE-2017-11930
MSKB	4053579
XREF	OSVDB:170718

XREF	OSVDB:170721
XREF	OSVDB:170722
XREF	OSVDB:170723
XREF	OSVDB:170724
XREF	OSVDB:170725
XREF	OSVDB:170727
XREF	OSVDB:170728
XREF	OSVDB:170729
XREF	OSVDB:170730
XREF	OSVDB:170731
XREF	OSVDB:170732
XREF	OSVDB:170733
XREF	OSVDB:170734
XREF	OSVDB:170735
XREF	OSVDB:170736
XREF	OSVDB:170737
XREF	OSVDB:170738
XREF	OSVDB:170739
XREF	OSVDB:170740
XREF	OSVDB:170741
XREF	OSVDB:170742
XREF	OSVDB:170743
XREF	OSVDB:170744
XREF	OSVDB:170745
XREF	MSFT:MS17-4053579

Plugin Information:

Published: 2017/12/12, Modified: 2018/01/15

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4053579

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.1944
```

105189 (1) - Security Updates for Microsoft Office Products (December 2017)

Synopsis

The Microsoft Office Products are missing a security update.

Description

The Microsoft Office Products are missing a security update.

It is, therefore, affected by the following vulnerability :

- An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the users computer or data. (CVE-2017-11934)

See Also

http://www.nessus.org/u?d5becb1c

http://www.nessus.org/u?831083d7

http://www.nessus.org/u?15e91184

Solution

Microsoft has released the following security updates to address this issue:

-KB4011612

-KB4011277

-KB4011095

Risk Factor

High

CVSS v3.0 Base Score

9.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

STIG Severity

II

References

CVE	CVE-2017-11934

MSKB	4011612
MSKB	4011277
MSKB	4011095
XREF	MSFT:MS17-4011612
XREF	MSFT:MS17-4011277
XREF	MSFT:MS17-4011095
XREF	IAVA:2017-A-0363

Plugin Information:

Published: 2017/12/12, Modified: 2017/12/15

Plugin Output

192.168.1.2 (tcp/445)

```
Product : Microsoft Office 2010 SP2
KB      : 4011612
- C:\Program Files (x86)\Microsoft Office\Office14\wwlib.dll has not been patched.
  Remote version : 14.0.7182.5000
  Should be      : 14.0.7191.5000
```

105192 (1) - Security Updates for Microsoft Word Products (December 2017)

Synopsis

The Microsoft Word Products are affected by multiple vulnerabilities.

Description

The Microsoft Word Products are missing security updates. Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure. The update disables the Dynamic Update Exchange protocol (DDE) in all supported editions of Microsoft Word. More information can be found in Microsoft Security Advisory 4053440.

See Also

http://www.nessus.org/u?e17d43f2

http://www.nessus.org/u?4ceb21ee

http://www.nessus.org/u?82734374

http://www.nessus.org/u?affd3524

http://www.nessus.org/u?314d33a5

Solution

Microsoft has released the following security updates to address this issue:

-KB4011590

-KB4011608

-KB4011614

-KB4011575

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

STIG Severity

II

References

MSKB	4011590
MSKB	4011608
MSKB	4011614
MSKB	4011575
XREF	MSFT:MS17-4011590
XREF	MSFT:MS17-4011608
XREF	MSFT:MS17-4011614
XREF	MSFT:MS17-4011575
XREF	IAVA:2017-A-0363

Plugin Information:

Published: 2017/12/12, Modified: 2017/12/15

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Word 2010
- C:\Program Files (x86)\Microsoft Office\Office14\WinWord.exe has not been patched.
  Remote version    : 14.0.7182.5000
  Fixed version     : 14.0.7191.5000
```

105356 (1) - Google Chrome < 63.0.3239.108 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 63.0.3239.108. It is, therefore, affected by multiple vulnerabilities as noted in Chrome stable channel update release notes for Thursday, December 14, 2017. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?125c6f30

Solution

Upgrade to Google Chrome version 63.0.3239.108 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102196
CVE	CVE-2017-15429
XREF	OSVDB:170937

XREF OSVDB:170938

Plugin Information:

Published: 2017/12/18, Modified: 2018/02/01

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 63.0.3239.108
```

105548 (1) - KB4056890: Windows 10 Version 1607 and Windows Server 2016 January 2018 Security Update (Meltdown)(Spectre)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 4056890 or 4057142. It is, therefore, affected by multiple vulnerabilities :

- An vulnerability exists within microprocessors utilizing speculative execution and indirect branch prediction, which may allow an attacker with local user access to disclose information via a side-channel analysis.

(CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)

- An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0744)

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2018-0758, CVE-2018-0769, CVE-2018-0770, CVE-2018-0776, CVE-2018-0777, CVE-2018-0781)

- An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. (CVE-2018-0746, CVE-2018-0747)

- An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. (CVE-2018-0803)

- An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. (CVE-2018-0754)

- A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

(CVE-2018-0762, CVE-2018-0772)

- An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2018-0766)

- An elevation of privilege vulnerability exists in the way that the Windows Kernel API enforces permissions. An attacker who successfully exploited the vulnerability could impersonate processes, interject cross-process communication, or interrupt system functionality.

(CVE-2018-0748, CVE-2018-0751, CVE-2018-0752)

- An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. (CVE-2018-0767, CVE-2018-0780)

- An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine. An attacker who successfully exploited this vulnerability could bypass certain security checks in the operating system. (CVE-2018-0749)

- A denial of service vulnerability exists in the way that Windows handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. Note that the denial of service condition would not allow an attacker to execute code or to elevate user privileges. However, the denial of service condition could prevent authorized users from using system resources. The security update addresses the vulnerability by correcting how Windows handles objects in memory. (CVE-2018-0753)

See Also

http://www.nessus.org/u?6dea4646

http://www.nessus.org/u?15261efc

https://support.microsoft.com/en-us/help/4072699

Solution

Apply Cumulative Update KB4056890 or KB4057142.

Notes:

- Due to a compatibility issue with some antivirus software products, it may not be possible to apply the required updates.

See Microsoft KB article 4072699 for more information.

- KB4057142 Addresses an issue with KB4056890 where some customers on a small subset of older AMD processors get into an unbootable state.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:ND)

STIG Severity

I

References

BID	102378
CVE	CVE-2017-5715
CVE	CVE-2017-5753
CVE	CVE-2017-5754
CVE	CVE-2018-0744
CVE	CVE-2018-0746
CVE	CVE-2018-0747
CVE	CVE-2018-0748
CVE	CVE-2018-0749
CVE	CVE-2018-0751
CVE	CVE-2018-0752
CVE	CVE-2018-0753
CVE	CVE-2018-0754
CVE	CVE-2018-0758
CVE	CVE-2018-0762
CVE	CVE-2018-0766
CVE	CVE-2018-0767
CVE	CVE-2018-0769
CVE	CVE-2018-0770
CVE	CVE-2018-0772
CVE	CVE-2018-0776
CVE	CVE-2018-0777
CVE	CVE-2018-0780
CVE	CVE-2018-0781
CVE	CVE-2018-0803
MSKB	4056890
MSKB	4057142
XREF	OSVDB:171888
XREF	OSVDB:171894
XREF	OSVDB:171897
XREF	OSVDB:171959

XREF	OSVDB:171963
XREF	OSVDB:171964
XREF	OSVDB:171966
XREF	OSVDB:171967
XREF	OSVDB:171970
XREF	OSVDB:171971
XREF	OSVDB:171976
XREF	OSVDB:171977
XREF	OSVDB:171978
XREF	OSVDB:171979
XREF	OSVDB:171980
XREF	OSVDB:171981
XREF	OSVDB:171983
XREF	OSVDB:171984
XREF	OSVDB:172008
XREF	OSVDB:172010
XREF	OSVDB:172011
XREF	OSVDB:172012
XREF	OSVDB:172013
XREF	OSVDB:172015
XREF	IAVA:2018-A-0019
XREF	IAVA:2018-A-0020
XREF	MSFT:MS18-4056890
XREF	MSFT:MS18-4057142

Plugin Information:

Published: 2018/01/04, Modified: 2018/02/15

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host is missing one of the following rollup KBs :
  - 4056890
  - 4057142

C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.14393.1480
    Should be      : 10.0.14393.2007
```

105691 (1) - Adobe Flash Player <= 28.0.0.126 (APSB18-01)

Synopsis

The remote Windows host has a browser plugin installed that is affected by an out-of-bounds read vulnerability.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 28.0.0.126. It is, therefore, affected by a an out-of-bounds read vulnerability.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb18-01.html

Solution

Upgrade to Adobe Flash Player version 28.0.0.137 or later.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102465
CVE	CVE-2018-4871
XREF	OSVDB:172249

Plugin Information:

Published: 2018/01/09, Modified: 2018/02/08

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 28.0.0.137
```

105693 (1) - KB4056887: Security update for Adobe Flash Player (January 2018)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4056887. It is, therefore, affected by a an out-of-bounds read vulnerability.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb18-01.html

http://www.nessus.org/u?d0e603fd

Solution

Microsoft has released KB4056887 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102465
CVE	CVE-2018-4871
MSKB	4056887
XREF	OSVDB:172249
XREF	MSFT:MS17-4056887

Plugin Information:

Published: 2018/01/09, Modified: 2018/02/08

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 28.0.0.137

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

105694 (1) - Security Updates for Microsoft Excel Products (January 2018)

Synopsis

The Microsoft Excel Products are affected by a remote code execution vulnerability.

Description

The Microsoft Excel Products are missing a security update.

It is, therefore, affected by the following vulnerability :

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0796)

See Also

http://www.nessus.org/u?01001d0d

http://www.nessus.org/u?a5dd4608

http://www.nessus.org/u?06c16d3c

http://www.nessus.org/u?c624d784

Solution

Microsoft has released the following security updates to address this issue:

-KB4011602

-KB4011627

-KB4011639

-KB4011660

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	102372
CVE	CVE-2018-0796
MSKB	4011602
MSKB	4011627
MSKB	4011639
MSKB	4011660
XREF	OSVDB:172274
XREF	MSFT:MS17-4011602
XREF	MSFT:MS17-4011627
XREF	MSFT:MS17-4011639
XREF	MSFT:MS17-4011660
XREF	IAVA:2018-A-0009

Plugin Information:

Published: 2018/01/09, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Excel 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe has not been patched.
  Remote version    : 14.0.7183.5000
  Fixed version     : 14.0.7192.5000
```

105699 (1) - Security Updates for Outlook (January 2018)

Synopsis

The version of Outlook installed on the remote host is affected by a remote code execution vulnerability.

Description

The version of Microsoft Outlook installed on the remote host is missing a security update. It is, therefore, affected by a remote code execution vulnerability in the way that Microsoft Outlook parses specially crafted email messages. An attacker who successfully exploited the vulnerability could take control of an affected system, then install programs; view, change, or delete data; or create new accounts with full user rights.

See Also

http://www.nessus.org/u?b69062a0

http://www.nessus.org/u?1ac0f408

http://www.nessus.org/u?e3387b83

http://www.nessus.org/u?8ad5d59d

Solution

Microsoft has released a set of patches for Outlook 2007, 2010, 2013, and 2016.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	102383
CVE	CVE-2018-0791
MSKB	4011213
MSKB	4011273
MSKB	4011637
MSKB	4011626
XREF	OSVDB:172256
XREF	MSFT:MS18-4011213
XREF	MSFT:MS18-4011273
XREF	MSFT:MS18-4011637
XREF	MSFT:MS18-4011626
XREF	IAVA:2018-A-0009

Plugin Information:

Published: 2018/01/09, Modified: 2018/01/11

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Outlook 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Outlook.exe has not been patched.
  Remote version    : 14.0.7187.5000
  Fixed version     : 14.0.7192.5000
```

105700 (1) - Security Updates for Microsoft Word Products (January 2018)

Synopsis

The Microsoft Word Products are affected by multiple vulnerabilities.

Description

The Microsoft Words Products are missing security updates. It is therefore affected by multiple issues involving handling of Office and RTF (Rich Text Format) files. If successfully exploited, an attacker could execute code in the context of the current user.

See Also

http://www.nessus.org/u?5ebcb266

http://www.nessus.org/u?3daf94ea

http://www.nessus.org/u?2ceece7f

http://www.nessus.org/u?66c1727d

Solution

Microsoft has released the following security updates to address this issue:

-KB4011657

-KB4011659

-KB4011651

-KB4011643

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	102370
BID	102373
BID	102375
BID	102381
BID	102406
CVE	CVE-2018-0792
CVE	CVE-2018-0793
CVE	CVE-2018-0794
CVE	CVE-2018-0797
CVE	CVE-2018-0798
CVE	CVE-2018-0845
CVE	CVE-2018-0848
CVE	CVE-2018-0849
CVE	CVE-2018-0862
MSKB	4011657
MSKB	4011643
MSKB	4011659
MSKB	4011651
XREF	OSVDB:172257
XREF	OSVDB:172258
XREF	OSVDB:172272
XREF	OSVDB:172275
XREF	OSVDB:172277
XREF	OSVDB:173186
XREF	OSVDB:173187
XREF	OSVDB:173188
XREF	OSVDB:173189
XREF	MSFT:MS18-4011657
XREF	MSFT:MS18-4011643
XREF	MSFT:MS18-4011659
XREF	MSFT:MS18-4011651
XREF	IAVA:2018-A-0009

Plugin Information:

Published: 2018/01/09, Modified: 2018/01/24

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Word 2010
- C:\Program Files (x86)\Microsoft Office\Office14\WinWord.exe has not been patched.
  Remote version    : 14.0.7182.5000
  Fixed version     : 14.0.7192.5000
```

105728 (1) - Security Updates for Microsoft Office Products (January 2018)

Synopsis

The Microsoft Office Products are missing a security update.

Description

The Microsoft Office Products are missing security updates.

It is, therefore, affected by the following vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0794, CVE-2018-0795)

- An Office RTF remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle RTF files. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0797)

- A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0798, CVE-2018-0801, CVE-2018-0802, CVE-2018-0804, CVE-2018-0805, CVE-2018-0806, CVE-2018-0807, CVE-2018-0812)

- A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially crafted email messages. An attacker who successfully exploited the vulnerability could take control of an affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook. (CVE-2018-0793)

See Also

http://www.nessus.org/u?e1b2b6d9

http://www.nessus.org/u?85b6869a

http://www.nessus.org/u?7d51c8cf

http://www.nessus.org/u?e7a15426

http://www.nessus.org/u?00956959

http://www.nessus.org/u?40ab628d

http://www.nessus.org/u?7cb9348d

http://www.nessus.org/u?479ec626

http://www.nessus.org/u?cf086d09

http://www.nessus.org/u?2b10eed9

Solution

Microsoft has released the following security updates to address this issue:

-KB4011201

-KB4011574

-KB4011580

-KB4011610

-KB4011611

-KB4011622

-KB4011632

-KB4011636

-KB4011656

-KB4011658

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.1 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

I

References

BID	102347
BID	102348
BID	102356
BID	102370
BID	102373
BID	102375

BID	102406
BID	102457
BID	102459
BID	102460
BID	102461
BID	102463
CVE	CVE-2018-0793
CVE	CVE-2018-0794
CVE	CVE-2018-0795
CVE	CVE-2018-0797
CVE	CVE-2018-0798
CVE	CVE-2018-0801
CVE	CVE-2018-0802
CVE	CVE-2018-0804
CVE	CVE-2018-0805
CVE	CVE-2018-0806
CVE	CVE-2018-0807
CVE	CVE-2018-0812
CVE	CVE-2018-0845
CVE	CVE-2018-0848
CVE	CVE-2018-0849
CVE	CVE-2018-0862
MSKB	4011201
MSKB	4011574
MSKB	4011580
MSKB	4011610
MSKB	4011611
MSKB	4011622
MSKB	4011632
MSKB	4011636
MSKB	4011656
MSKB	4011658
XREF	OSVDB:172258
XREF	OSVDB:172264
XREF	OSVDB:172265
XREF	OSVDB:172266
XREF	OSVDB:172267
XREF	OSVDB:172268
XREF	OSVDB:172270
XREF	OSVDB:172271
XREF	OSVDB:172272
XREF	OSVDB:172273
XREF	OSVDB:172275

XREF	OSVDB:172277
XREF	OSVDB:173186
XREF	OSVDB:173187
XREF	OSVDB:173188
XREF	OSVDB:173189
XREF	MSFT:MS17-4011201
XREF	MSFT:MS17-4011574
XREF	MSFT:MS17-4011580
XREF	MSFT:MS17-4011610
XREF	MSFT:MS17-4011611
XREF	MSFT:MS17-4011622
XREF	MSFT:MS17-4011632
XREF	MSFT:MS17-4011636
XREF	MSFT:MS17-4011656
XREF	MSFT:MS17-4011658
XREF	IAVA:2018-A-0009

Exploitable With

Core Impact (true)

Plugin Information:

Published: 2018/01/10, Modified: 2018/02/07

Plugin Output

192.168.1.2 (tcp/445)

```
Product : Microsoft Office 2010 SP2
KB      : 4011611
- C:\Program Files (x86)\Common Files\Microsoft Shared\Office14\mso.dll has not been patched.
  Remote version : 14.0.7184.5000
  Should be      : 14.0.7192.5000

Product : Microsoft Office 2010 SP2
KB      : 4011610
- C:\Program Files (x86)\Common Files\Microsoft Shared\Equation\eqnedt32.exe has not been patched.
  Remote version : 2000.11.9.0
  Should be      : 2018.0.0.0
```

106350 (1) - Google Chrome < 62.0.3202.94 Out of bounds read flaw in V8

Synopsis

A web browser installed on the remote Windows host is affected by an out of bounds read flaw in the V8 component of Google Chrome.

Description

The version of Google Chrome installed on the remote Windows host is prior to 62.0.3202.94. It is, therefore, affected by an out of bounds read flaw in V8 as noted in Chrome stable channel update release notes for November 13th, 2017. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?19ef0025

Solution

Upgrade to Google Chrome version 62.0.3202.94 or later.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-15428
XREF	OSVDB:173221

Plugin Information:

Published: 2018/01/25, Modified: 2018/01/29

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 62.0.3202.94
```

106485 (1) - Google Chrome < 64.0.3282.119 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple security vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 64.0.3282.119. It is, therefore, affected by multiple security vulnerabilities as noted in Chrome stable channel update release notes for January 24th, 2018. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?26e44d0b

Solution

Upgrade to Google Chrome version 64.0.3282.119 or later.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

CVSS Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102098
CVE	CVE-2017-15420
CVE	CVE-2018-6031
CVE	CVE-2018-6032
CVE	CVE-2018-6033
CVE	CVE-2018-6034
CVE	CVE-2018-6035

CVE	CVE-2018-6036
CVE	CVE-2018-6037
CVE	CVE-2018-6038
CVE	CVE-2018-6039
CVE	CVE-2018-6040
CVE	CVE-2018-6041
CVE	CVE-2018-6042
CVE	CVE-2018-6043
CVE	CVE-2018-6045
CVE	CVE-2018-6046
CVE	CVE-2018-6047
CVE	CVE-2018-6048
CVE	CVE-2018-6049
CVE	CVE-2018-6050
CVE	CVE-2018-6051
CVE	CVE-2018-6052
CVE	CVE-2018-6053
CVE	CVE-2018-6054
XREF	OSVDB:170416
XREF	OSVDB:173453
XREF	OSVDB:173454
XREF	OSVDB:173455
XREF	OSVDB:173456
XREF	OSVDB:173457
XREF	OSVDB:173458
XREF	OSVDB:173459
XREF	OSVDB:173460
XREF	OSVDB:173461
XREF	OSVDB:173462
XREF	OSVDB:173463
XREF	OSVDB:173464
XREF	OSVDB:173465
XREF	OSVDB:173466
XREF	OSVDB:173467
XREF	OSVDB:173468
XREF	OSVDB:173469
XREF	OSVDB:173471
XREF	OSVDB:173472
XREF	OSVDB:173473
XREF	OSVDB:173474
XREF	OSVDB:173475
XREF	OSVDB:173510
XREF	OSVDB:175024

Plugin Information:

Published: 2018/01/30, Modified: 2018/02/20

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 64.0.3282.119
```

106606 (1) - Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) (APSB18-03)

Synopsis

The remote Windows host has a browser plugin installed that is affected by a remote code execution vulnerability.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 28.0.0.137. It is, therefore, affected by a use-after-free vulnerability that allows arbitrary code execution.

See Also

https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

https://helpx.adobe.com/security/products/flash-player/apsb18-03.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 28.0.0.161 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.1 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	102893
BID	102930

CVE	CVE-2018-4877
CVE	CVE-2018-4878
XREF	OSVDB:173919
XREF	OSVDB:174144

Plugin Information:

Published: 2018/02/05, Modified: 2018/03/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product : ActiveX control (for Internet Explorer)
 Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
 Installed version : 26.0.0.137
 Fixed version     : 28.0.0.161
```

106655 (1) - KB4074595: Security update for Adobe Flash Player (February 2018)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4074595. It is, therefore, affected by multiple remote code execution vulnerabilities in Adobe Flash Player.

See Also

https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

https://helpx.adobe.com/security/products/flash-player/apsb18-03.html

http://www.nessus.org/u?9e60077b

Solution

Microsoft has released KB4074595 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.1 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.7 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	102893
BID	102930
CVE	CVE-2018-4877
CVE	CVE-2018-4878

MSKB	4074595
XREF	OSVDB:173919
XREF	OSVDB:174144
XREF	MSFT:MS18-4074595

Plugin Information:

Published: 2018/02/07, Modified: 2018/03/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 28.0.0.161

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

106805 (1) - Security Updates for Microsoft Office Products (February 2018)

Synopsis

The Microsoft Office Products are missing a security update.

Description

The Microsoft Office Products are missing security updates.

It is, therefore, affected by the following vulnerabilities :

- A remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0851)

- An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory. An attacker who successfully exploited the vulnerability could view out of bound memory. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. The security update addresses the vulnerability by properly initializing the affected variable. (CVE-2018-0853)

See Also

http://www.nessus.org/u?d7092ec1

http://www.nessus.org/u?25ea79c7

http://www.nessus.org/u?7216394c

http://www.nessus.org/u?eec18988

http://www.nessus.org/u?c68f10e8

http://www.nessus.org/u?2d37ad2f

http://www.nessus.org/u?0bc5ff1d

Solution

Microsoft has released the following security updates to address this issue:

-KB4011715

-KB4011707

-KB3114874

-KB4011690

-KB3172459

-KB4011686

-KB4011143

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2018-0851
CVE	CVE-2018-0853
MSKB	4011715
MSKB	4011707
MSKB	3114874
MSKB	4011690
MSKB	3172459
MSKB	4011686
MSKB	4011143
XREF	OSVDB:174895
XREF	MSFT:MS18-4011715
XREF	MSFT:MS18-4011707
XREF	MSFT:MS18-3114874
XREF	MSFT:MS18-4011690
XREF	MSFT:MS18-3172459
XREF	MSFT:MS18-4011686
XREF	MSFT:MS18-4011143
XREF	IAVA:2018-A-0051

Plugin Information:

Published: 2018/02/13, Modified: 2018/02/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product : Microsoft Office 2010 SP2
KB      : 4011707
- C:\Program Files (x86)\Common Files\Microsoft Shared\Office14\mso.dll has not been patched.
  Remote version : 14.0.7184.5000
  Should be      : 14.0.7194.5000

Product : Microsoft Office 2010 SP2
KB      : 3114874
- C:\Program Files (x86)\Common Files\Microsoft Shared\Office14\acecore.dll has not been patched.
  Remote version : 14.0.7159.5000
  Should be      : 14.0.7194.5000
```

106807 (1) - Security Updates for Outlook (February 2018)

Synopsis

The Microsoft Outlook application installed on the remote host is affected by multiple vulnerabilities.

Description

The Microsoft Outlook application installed on the remote host is missing security updates. It is, therefore, affected by multiple vulnerabilities :

- An elevation of privilege vulnerability exists when Microsoft Outlook initiates processing of incoming messages without sufficient validation of the formatting of the messages. An attacker who successfully exploited the vulnerability could attempt to force Outlook to load a local or remote message store (over SMB).

(CVE-2018-0850)

- A remote code execution vulnerability exists in Microsoft Outlook when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

(CVE-2018-0852)

See Also

http://www.nessus.org/u?f0d84fef

http://www.nessus.org/u?4444a3b8

http://www.nessus.org/u?13b4a7cf

http://www.nessus.org/u?7de39c82

Solution

Microsoft has released the following security updates to address this issue:

- KB4011682
- KB4011697
- KB4011711
- KB4011200

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	102866
BID	102871
CVE	CVE-2018-0850
CVE	CVE-2018-0852
MSKB	4011682
MSKB	4011697
MSKB	4011711
MSKB	4011200
XREF	OSVDB:174896
XREF	OSVDB:174903
XREF	OSVDB:174904
XREF	MSFT:MS18-4011682
XREF	MSFT:MS18-4011697
XREF	MSFT:MS18-4011711
XREF	MSFT:MS18-4011200
XREF	IAVA:2018-A-0051

Plugin Information:

Published: 2018/02/13, Modified: 2018/02/21

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Outlook 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Outlook.exe has not been patched.
  Remote version    : 14.0.7187.5000
  Fixed version     : 14.0.7194.5000
```

106840 (1) - Google Chrome < 64.0.3282.167 V8 JSFunction::CalculateInstanceSizeForDerivedClass() RCE

Synopsis

A web browser installed on the remote Windows host is affected by a code execution vulnerability.

Description

The version of Google Chrome installed on the remote Windows host is prior to 64.0.3282.167. It is, therefore, affected by a flaw in the V8 JavaScript engine as noted in Chrome stable channel update release notes for February 13th, 2018. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?7f96d3ea

Solution

Upgrade to Google Chrome version 64.0.3282.167 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	103003
CVE	CVE-2018-6056

XREF OSVDB:174922

Plugin Information:

Published: 2018/02/15

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 64.0.3282.167
```

107220 (1) - Google Chrome < 65.0.3325.146 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote Windows host is prior to 65.0.3325.146. It is, therefore, affected by a multiple unspecified vulnerabilities as noted in Chrome stable channel update release notes for March 6th, 2018. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?68129919

Solution

Upgrade to Google Chrome version 65.0.3325.146 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	101837
CVE	CVE-2017-11215
CVE	CVE-2017-11225

CVE	CVE-2018-6057
CVE	CVE-2018-6060
CVE	CVE-2018-6061
CVE	CVE-2018-6062
CVE	CVE-2018-6063
CVE	CVE-2018-6064
CVE	CVE-2018-6065
CVE	CVE-2018-6066
CVE	CVE-2018-6067
CVE	CVE-2018-6068
CVE	CVE-2018-6069
CVE	CVE-2018-6070
CVE	CVE-2018-6071
CVE	CVE-2018-6072
CVE	CVE-2018-6073
CVE	CVE-2018-6074
CVE	CVE-2018-6075
CVE	CVE-2018-6076
CVE	CVE-2018-6077
CVE	CVE-2018-6078
CVE	CVE-2018-6079
CVE	CVE-2018-6080
CVE	CVE-2018-6081
CVE	CVE-2018-6082
CVE	CVE-2018-6083
XREF	OSVDB:169127
XREF	OSVDB:169128
XREF	OSVDB:176182
XREF	OSVDB:176183
XREF	OSVDB:176184
XREF	OSVDB:176185
XREF	OSVDB:176186
XREF	OSVDB:176187
XREF	OSVDB:176188
XREF	OSVDB:176189
XREF	OSVDB:176190
XREF	OSVDB:176191
XREF	OSVDB:176192
XREF	OSVDB:176193
XREF	OSVDB:176194
XREF	OSVDB:176195
XREF	OSVDB:176196
XREF	OSVDB:176197

XREF	OSVDB:176198
XREF	OSVDB:176199
XREF	OSVDB:176200
XREF	OSVDB:176201
XREF	OSVDB:176202
XREF	OSVDB:176203
XREF	OSVDB:176204
XREF	OSVDB:176205
XREF	OSVDB:176207
XREF	IAVA:2018-A-0070

Plugin Information:

Published: 2018/03/08, Modified: 2018/03/13

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 65.0.3325.146
```

108281 (1) - Adobe Flash Player <= 28.0.0.161 (APSB18-05)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 28.0.0.161. It is therefore affected by multiple vulnerabilities.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb18-05.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 29.0.0.113 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

CVE	CVE-2018-4919
CVE	CVE-2018-4920
XREF	IAVA:2018-A-0071

Plugin Information:

Published: 2018/03/13, Modified: 2018/03/16

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 29.0.0.113
```

108287 (1) - KB4088785: Security update for Adobe Flash Player (March 2018)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4088785. It is, therefore, affected by multiple remote code execution vulnerabilities in Adobe Flash Player.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb18-05.html

http://www.nessus.org/u?277368d9

Solution

Microsoft has released KB4088785 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

BID	103385
BID	103383
CVE	CVE-2018-4919
CVE	CVE-2018-4920
MSKB	4088785
XREF	OSVDB:176604
XREF	OSVDB:176605
XREF	IAVA:2018-A-0071
XREF	MSFT:MS18-4088785

XREF IAVA:2018-A-0071

Plugin Information:

Published: 2018/03/13, Modified: 2018/03/22

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 29.0.0.113

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

108301 (1) - Security Updates for Microsoft Word Products (March 2018)

Synopsis

The Microsoft Word Products are affected by multiple vulnerabilities.

Description

The Microsoft Word Products are missing security updates. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory. An attacker who successfully exploited the vulnerability could view out of bound memory. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. The security update addresses the vulnerability by properly initializing the affected variable. (CVE-2018-0919)

- A remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2018-0922)

See Also

http://www.nessus.org/u?a931ed8a

http://www.nessus.org/u?28553b79

http://www.nessus.org/u?37a5148f

http://www.nessus.org/u?797b3826

Solution

Microsoft has released the following security updates to address this issue:

-KB4011721

-KB4011674

-KB4011730

-KB4011695

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

BID	103311
BID	103314
CVE	CVE-2018-0919
CVE	CVE-2018-0922
MSKB	4011721
MSKB	4011674
MSKB	4011730
MSKB	4011695
XREF	OSVDB:176690
XREF	OSVDB:176691
XREF	IAVA:2018-A-0077
XREF	MSFT:MS18-4011721
XREF	MSFT:MS18-4011674
XREF	MSFT:MS18-4011730
XREF	MSFT:MS18-4011695
XREF	IAVA:2018-A-0077

Plugin Information:

Published: 2018/03/13, Modified: 2018/03/22

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Word 2010
- C:\Program Files (x86)\Microsoft Office\Office14\WinWord.exe has not been patched.
  Remote version    : 14.0.7182.5000
  Fixed version     : 14.0.7195.5000
```

63155 (1) - Microsoft Windows Unquoted Service Path Enumeration

Synopsis

The remote Windows host has at least one service installed that uses an unquoted service path.

Description

The remote Windows host has at least one service installed that uses an unquoted service path, which contains at least one whitespace. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service.

Note that this is a generic test that will flag any application affected by the described vulnerability.

See Also

http://www.nessus.org/u?84a4cc1c

http://cwe.mitre.org/data/definitions/428.html

https://www.commonexploits.com/unquoted-service-paths/

http://www.nessus.org/u?4aa6acbc

Solution

Ensure that any services that contain a space in the path enclose the path in quotes.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:F/RL:X/RC:X)

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.6 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	58591

BID	58617
BID	65873
BID	68520
CVE	CVE-2013-1609
CVE	CVE-2014-0759
CVE	CVE-2014-5455
XREF	OSVDB:91492
XREF	OSVDB:91582
XREF	OSVDB:102505
XREF	OSVDB:109007
XREF	OSVDB:132967
XREF	ICSA:14-058-01
XREF	EDB-ID:34037

Exploitable With

Metasploit (true)

Plugin Information:

Published: 2012/12/05, Modified: 2017/03/28

Plugin Output

192.168.1.2 (tcp/445)

```
Nessus found the following service with an untrusted path :
  NasPmService : C:\Program Files (x86)\BUFFALO\NASNAVI\nassvc.exe
```

73992 (1) - MS KB2960358: Update for Disabling RC4 in .NET TLS

Synopsis

The remote host has a deprecated, weak encryption cipher available.

Description

The remote host is missing an update for disabling the weak RC4 cipher suite in .NET TLS.

Note that even though .NET Framework 4.6 itself is not affected, any Framework 4.5, 4.5.1, or 4.5.2 application that runs on a system that has 4.6 installed is affected.

See Also

https://technet.microsoft.com/library/security/2960358

Solution

Microsoft has released a set of security updates for the .NET Framework on Windows 7, 2008 R2, 8, 2012, 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

References

MSKB	2960358

Plugin Information:

Published: 2015/10/13, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/445)

```
The following registry values have not been
set to 1 :
HKLM\SOFTWARE\Microsoft\.NETFramework\v2.0.50727\SchUseStrongCrypto
HKLM\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\SchUseStrongCrypto
```

100056 (1) - Security and Quality Rollup for .NET Framework (May 2017)

Synopsis

The remote Windows host has a software framework installed that is affected by a security feature bypass vulnerability.

Description

The version of Microsoft .NET Framework installed on the remote Windows host is missing a security update. It is, therefore, affected by a security bypass vulnerability in the Microsoft .NET Framework and .NET Core components due to a failure to completely validate certificates. An unauthenticated, remote attacker can exploit this to present a certificate that is marked invalid for a specific use, but the component uses it for that purpose, resulting in a bypass of the Enhanced Key Usage taggings.

See Also

http://www.nessus.org/u?891ed5ca

http://www.nessus.org/u?e3805e39

Solution

Microsoft has released a set of patches for Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

BID	98117
CVE	CVE-2017-0248
MSKB	4016871
MSKB	4019108
MSKB	4019109
MSKB	4019110
MSKB	4019111
MSKB	4019112
MSKB	4019113
MSKB	4019114
MSKB	4019115
MSKB	4019472
MSKB	4019473
MSKB	4019474
XREF	OSVDB:157277
XREF	MSFT:MS17-4016871
XREF	MSFT:MS17-4019108
XREF	MSFT:MS17-4019109
XREF	MSFT:MS17-4019110
XREF	MSFT:MS17-4019111
XREF	MSFT:MS17-4019112
XREF	MSFT:MS17-4019113
XREF	MSFT:MS17-4019114
XREF	MSFT:MS17-4019115
XREF	MSFT:MS17-4019472
XREF	MSFT:MS17-4019473
XREF	MSFT:MS17-4019474
XREF	IAVB:2017-B-0055

Plugin Information:

Published: 2017/05/09, Modified: 2018/01/30

Plugin Output

192.168.1.2 (tcp/445)

```
Microsoft .NET Framework 3.5
The remote host is missing one of the following rollup KBs :
  - 4019472

C:\Windows\Microsoft.NET\Framework\v2.0.50727\system.dll has not been patched.
    Remote version : 2.0.50727.8745
    Should be      : 2.0.50727.8759
```

105175 (1) - Adobe Flash Player <= 27.0.0.187 (APSB17-42)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 27.0.0.187. It is, therefore, affected by a vulnerability which may allow an attacker to reset the global settings preference file.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-42.html

http://www.nessus.org/u?0cb17c10

Solution

Upgrade to Adobe Flash Player version 28.0.0.126 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102139
CVE	CVE-2017-11305
XREF	OSVDB:170675

Plugin Information:

Published: 2017/12/12, Modified: 2018/01/11

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : ActiveX control (for Internet Explorer)
Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
Installed version : 26.0.0.137
Fixed version     : 28.0.0.126
```

105178 (1) - KB4053577: Security update for Adobe Flash Player (December 2017)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update KB4053577. It is, therefore, affected by a vulnerability which may allow an attacker to reset the global settings preference file.

See Also

https://helpx.adobe.com/security/products/flash-player/apsb17-42.html

http://www.nessus.org/u?e94655ce

Solution

Microsoft has released KB4053577 to address this issue.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	102139
CVE	CVE-2017-11305
MSKB	4053577
XREF	OSVDB:170675
XREF	MSFT:MS17-4053577

Plugin Information:

Published: 2017/12/12, Modified: 2018/01/16

Plugin Output

192.168.1.2 (tcp/445)

```
  Path              : C:\Windows\System32\Macromed\Flash\Flash.ocx
  Installed version : 26.0.0.137
  Fixed version     : 28.0.0.126

Moreover, its kill bit is not set so it is accessible via Internet
Explorer.
```

106682 (1) - Google Chrome < 64.0.3282.140 V8 Factory::NewFunction() RCE

Synopsis

A web browser installed on the remote Windows host is affected by a code execution vulnerability.

Description

The version of Google Chrome installed on the remote Windows host is prior to 64.0.3282.140. It is, therefore, affected by a flaw in the V8 JavaScript engine as noted in Chrome stable channel update release notes for February 1st, 2018. Please refer to the release notes for additional information.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?205f733f

Solution

Upgrade to Google Chrome version 64.0.3282.140 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:P/RL:O/RC:X)

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

XREF	OSVDB:173920

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

192.168.1.2 (tcp/445)

```
Path              : C:\Program Files (x86)\Google\Chrome\Application
Installed version : 60.0.3112.113
Fixed version     : 64.0.3282.140
```

108293 (1) - Security Updates for Microsoft Excel Products (March 2018)

Synopsis

The Microsoft Excel Products are affected by a security feature bypass vulnerability.

Description

The Microsoft Excel Products are missing a security update.

It is, therefore, affected by the following vulnerability :

- A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Microsoft Office software. The security update addresses the vulnerability by enforcing macro settings on Excel documents.

(CVE-2018-0907)

See Also

http://www.nessus.org/u?5bf879e0

Solution

Microsoft has released the following security updates to address this issue:

-KB4011675

-KB4011714

-KB4011727

-KB4018291

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

STIG Severity

I

References

BID	103325
CVE	CVE-2018-0907
MSKB	4011675
MSKB	4011714
MSKB	4011727
MSKB	4018291
XREF	OSVDB:176668
XREF	IAVA:2018-A-0077
XREF	MSFT:MS18-4011675
XREF	MSFT:MS18-4011714
XREF	MSFT:MS18-4011727
XREF	MSFT:MS18-4018291
XREF	IAVA:2018-A-0077

Plugin Information:

Published: 2018/03/13, Modified: 2018/03/22

Plugin Output

192.168.1.2 (tcp/445)

```
Product           : Excel 2010
- C:\Program Files (x86)\Microsoft Office\Office14\Excel.exe has not been patched.
  Remote version    : 14.0.7183.5000
  Fixed version     : 14.0.7195.5000
```

11457 (1) - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0. Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).

See Also

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Use regedt32 and set the value of this registry key to 0.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Published: 2003/03/24, Modified: 2017/12/05

Plugin Output

192.168.1.2 (tcp/445)

```
Max cached logons : 10
```

10736 (8) - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

192.168.1.2 (tcp/135)

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0F2CC0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0F2CC0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE99C0EB4B31F6C71AAE4A80B90E46

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-062f73570846014f9c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 000002a2-fb3c-0007-4b50-525250524944
UUID : 000002a2-d801-7233-4b50-525250524f50, version 32.108
Description : Unknown RPC service
Annotation : PR_REMOTE_MANAGER_PROP
Type : Local RPC service
Named pipe : PRRNameService:9944

Object UUID : 000002a2-e72a-000f-4b50-525250524944
UUID : 000002a2-e474-f035-4b50-525250524f50, version 32.108
Description : Unknown RPC service
Annotation : cpnPRAGUE_REMOTE_API
Type : Local RPC service
Named pipe : PRRNameService:9944

Object UUID : 05497a28-0000-0000-4b50-5252484e444c
UUID : 000002a2-c75c-28ad-4b50-52524f424a53, version 32.108
Description  [...]
```

192.168.1.2 (tcp/445)

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\HOST-M05

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\HOST-M05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\HOST-M05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\HOST-M05
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\HOST-M05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\HOST-M05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\HOST-M05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\NE [...]
```

192.168.1.2 (tcp/49664)

```
The following DCERPC services are available on TCP port 49664 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.1.2
```

192.168.1.2 (tcp/49665)

```
The following DCERPC services are available on TCP port 49665 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
```

```
TCP Port : 49665
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.1.2
```

192.168.1.2 (tcp/49666)

```
The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
```

```
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unkno [...]
```

192.168.1.2 (tcp/49667)

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
```

```
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.1.2
```

192.168.1.2 (tcp/49668)

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.1.2
```

192.168.1.2 (tcp/49669)

```
The following DCERPC services are available on TCP port 49669 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.1.2
```

11219 (3) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

192.168.1.2 (tcp/135)

```
Port 135/tcp was found to be open
```

192.168.1.2 (tcp/139)

```
Port 139/tcp was found to be open
```

192.168.1.2 (tcp/445)

```
Port 445/tcp was found to be open
```

11011 (2) - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

192.168.1.2 (tcp/139)

```
An SMB server is running on this port.
```

192.168.1.2 (tcp/445)

```
A CIFS server is running on this port.
```

10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/09/27

Plugin Output

192.168.1.2 (udp/137)

```
The following 6 NetBIOS names have been gathered :

HOST-M05          = File Server Service
HOST-M05          = Computer name
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   f0:de:f1:3b:54:98
```

10394 (1) - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

https://support.microsoft.com/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2017/11/06

Plugin Output

192.168.1.2 (tcp/445)

```
- NULL sessions are enabled on the remote host.
- The SMB tests will be done as Administrator/******
```

10395 (1) - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
Here are the SMB shares available on the remote host when logged in as Administrator:

  - ADMIN$
  - C$
  - D$
  - IPC$
  - scan
  - Users
  - yaccbackup$
```

10396 (1) - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

References

CVE	CVE-1999-0519
CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Published: 2000/05/09, Modified: 2015/11/18

Plugin Output

192.168.1.2 (tcp/445)

```
The following shares can be accessed as Administrator :

- yaccbackup$  - (readable,writable)
  + Content of this share :
..

- Users  - (readable,writable)
  + Content of this share :
..
Administrator
All Users
Default
Default User
defaultuser0
desktop.ini
haruka
```

```
kamata
Public
yamada

- ADMIN$  - (readable,writable)
  + Content of this share :
..
addins
appcompat
AppPatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
BitLockerDiscoveryVolumeContents
Boot
bootstat.dat
Branding
CbsTemp
CSC
Cursors
debug
diagnostics
DigitalLocker
Downloaded Program Files
DtcInstall.log
ELAMBKUP
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IME
ImmersiveControlPanel
INF
InfusedApps
InputMethod
Installer
ja-JP
L2Schemas
Lhaca.ini
LiveKernelReports
Logs
lsasetup.log
Media
MEMORY.DMP
mib.bin
Microsoft.NET
Migration
Minidump
MiracastView
ModemLogs
notepad.exe
OCR
Offline Web Pages
Panther
PCHEALTH
Performance
PFRO.log
PLA
PolicyDefinitions
Prefetch
PrintDialog
Professional.xml
Provisioning
regedit.exe
registration
```

```
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
servicing
Setup
setupact.log
setuperr.log
ShellExperiences
SHELLNEW
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
SystemResources
SysWOW64
TAPI
Tasks
Temp
tracing
twain_32
twain_32.dll

- C$  - (readable,writable)
  + Content of this share :
bootmgr
BOOTNXT
BUFFALO
Documents and Settings
hiberfil.sys
Intel
MSOCache
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
scan
swapfile.sys
System Volume Information
Users
usr
Windows

- D$  - (readable,writable)
  + Content of this share :
MediaID.bin
HOST-M05
System Volume Information
WindowsImageBackup

- scan  - (readable,writable)
  + Content of this share :
..
```

10400 (1) - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

10456 (1) - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.

An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Published: 2000/07/03, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
Active Services :

Application Information [ Appinfo ]
App Readiness [ AppReadiness ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Kaspersky Endpoint Security Service [ AVP ]
Kaspersky Seamless Update Service [ avpsus ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Computer Browser [ Browser ]
Connected Devices Platform Service [ CDPSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Association Service [ DeviceAssociationService ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Device Setup Manager [ DsmSvc ]
Data Sharing Service [ DsSvc ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Function Discovery Resource Publication [ FDResPub ]
```

```
Windows Font Cache Service [ FontCache ]
Windows Presentation Foundation Font Cache 3.0.0.0 [ FontCache3.0.0.0 ]
HomeGroup Provider [ HomeGroupProvider ]
Lenovo PM Service [ IBMPMSVC ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
IP Helper [ iphlpsvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Geolocation Service [ lfsvc ]
Windows ..... ...... .... [ LicenseManager ]
TCP/IP NetBIOS Helper [ lmhosts ]
Lenovo Platform Service [ LPlatSvc ]
Local Session Manager [ LSM ]
Windows Firewall [ MpsSvc ]
NAS PM Service [ NasPmService ]
Network Connection Broker [ NcbService ]
Network Connections [ Netman ]
Network List Service [ netprofm ]
Network Location Awareness [ NlaSvc ]
Network Store Interface Service [ nsi ]
Office Software Protection Platform [ osppsvc ]
Program Compatibility Assistant Service [ PcaSvc ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
Remote Access Connection Manager [ RasMan ]
Remote Regi [...]
```

10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

192.168.1.2 (tcp/445)

```
The remote Operating System is : Windows 10 Pro 14393
The remote native LAN manager is : Windows 10 Pro 6.3
The remote SMB Domain Name is : HOST-M05
```

10859 (1) - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Plugin Information:

Published: 2002/02/13, Modified: 2015/11/18

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host SID value is :

1-5-21-2552265371-3243985514-2585313438

The value of 'RestrictAnonymous' setting is : 0
```

10860 (1) - SMB Use Host SID to Enumerate Local Users

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:714

Plugin Information:

Published: 2002/02/13, Modified: 2017/02/02

Plugin Output

192.168.1.2 (tcp/445)

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - DefaultAccount (id 503)
  - defaultuser0 (id 1000)
  - kamata (id 1001)
  - haruka (id 1003)
  - yamada (id 1004)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 500 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

10902 (1) - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Published: 2002/03/15, Modified: 2016/08/24

Plugin Output

192.168.1.2 (tcp/445)

```
The following users are members of the 'Administrators' group :

  - HOST-M05\Administrator (User)
  - HOST-M05\kamata (User)
  - HOST-M05\haruka (User)
```

10913 (1) - Microsoft Windows - Local Users Information : Disabled Accounts

Synopsis

At least one local user account has been disabled.

Description

Using the supplied credentials, Nessus was able to list local user accounts that have been disabled.

Solution

Delete accounts that are no longer needed.

Risk Factor

None

References

XREF OSVDB:752

Plugin Information:

Published: 2002/03/17, Modified: 2017/01/26

Plugin Output

192.168.1.2 (tcp/0)

```
The following local user accounts have been disabled :

  - DefaultAccount
  - defaultuser0


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 500 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10914 (1) - Microsoft Windows - Local Users Information : Never Changed Passwords

Synopsis

At least one local user has never changed his or her password.

Description

Using the supplied credentials, Nessus was able to list local users who have never changed their passwords.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

References

XREF OSVDB:755

Plugin Information:

Published: 2002/03/17, Modified: 2017/01/26

Plugin Output

192.168.1.2 (tcp/0)

```
The following local users have never changed their passwords :

  - Guest
  - DefaultAccount


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 500 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10915 (1) - Microsoft Windows - Local Users Information : User Has Never Logged In

Synopsis

At least one local user has never logged into his or her account.

Description

Using the supplied credentials, Nessus was able to list local users who have never logged into their accounts.

Solution

Delete accounts that are not needed.

Risk Factor

None

References

XREF OSVDB:754

Plugin Information:

Published: 2002/03/17, Modified: 2017/01/26

Plugin Output

192.168.1.2 (tcp/0)

```
The following local users have never logged in :

  - Guest
  - DefaultAccount


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 500 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10916 (1) - Microsoft Windows - Local Users Information : Passwords Never Expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

References

XREF OSVDB:755

Plugin Information:

Published: 2002/03/17, Modified: 2017/01/26

Plugin Output

192.168.1.2 (tcp/0)

```
The following local users have passwords that never expire :

  - Administrator
  - Guest
  - kamata
  - haruka


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 500 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

16193 (1) - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?b145ae41

http://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/01/18, Modified: 2017/09/05

Plugin Output

192.168.1.2 (tcp/445)

```
Kaspersky :
Kaspersky Anti-Virus is installed on the remote host :

  Product name      : Kaspersky Endpoint Security for Windows
  Version           : 10.2.5.3201
  Installation path : C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for
 Windows SP1\
  Virus signatures  : 09/09/2017

The virus signatures on the remote host are out-of-date - the last
known update from the vendor is 04/03/2018
```

17651 (1) - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

192.168.1.2 (tcp/0)

```
Information about this scan :

Nessus version : 7.0.3
Plugin feed version : 201804032215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Credentialed Patch Audit
Scanner IP : 192.168.1.70
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as '192.168.1.2\Administrator' via SMB
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/4/5 11:52 JST
Scan duration : 559 sec
```

20811 (1) - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates

Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2006/01/26, Modified: 2013/07/25

Plugin Output

192.168.1.2 (tcp/445)

```
The following software are installed on the remote host :

Becky! Ver.2  [installed on 2017/05/04]
Conexant 20585 SmartAudio HD  [version 4.95.49.53]
Google Chrome  [version 60.0.3112.113]  [installed on 2017/05/04]
Kyocera Product Library  [version 5.0.1120]
+Lhaca
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)  [version 10.0.50903]
Microsoft Visual Studio 2010 Tools for Office Runtime (x64) Language Pack - .,.  [version
 10.0.50903]
Microsoft Office Standard 2010  [version 14.0.7015.1000]
Lenovo Power Management Driver  [version 1.67.12.19]
Synaptics Pointing Device Driver  [version 19.0.16.0]
TeamViewer 10  [version 10.0.47484]
BUFFALO NAS Navigator2  [version .2.90]
Microsoft Visual Studio Team Foundation Server 2017 Office Integration (x64)  [version 15.112.26322]
  [installed on 2017/04/14]
icecap_collection_x64  [version 15.0.26208]  [installed on 2017/04/14]
vs_BlendMsi  [version 15.0.26208]  [installed on 2017/04/14]
vs_FileTracker_Singleton  [version 15.0.26208]  [installed on 2017/04/14]
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005  [version 12.0.21005]  [installed on
 2017/08/28]
vs_filehandler_amd64  [version 15.0.26228]  [installed on 2017/04/14]
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501  [version 12.0.30501.0]
Microsoft .NET Framework 4.5.2 Multi-Targeting Pack  [version 4.5.51651]  [installed on 2017/04/14]
```

```
Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219  [version 10.0.40219]  [installed on
 2017/05/04]
VS JIT Debugger  [version 16.0.59.0]  [installed on 2017/04/14]
Microsoft .NET Framework 4.6 Targeting Pack  [version 4.6.00081]  [installed on 2017/04/14]
Microsoft .NET Framework 4.6.1 SDK  [version 4.6.01055]  [installed on 2017/04/14]
Microsoft .NET Framework Cumulative Intellisense Pack for Visual Studio (.,.)  [version 4.6.01604]
 [installed on 2017/04/14]
Microsoft Visual Studio Team Foundation Server 2017 Office Integration Language Pack (x64) - ENU
 [version 15.112.26322]  [installed on 2017/04/14]
Windows 10 Update and Privacy Settings [...]
```

23974 (1) - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information:

Published: 2007/01/04, Modified: 2011/03/21

Plugin Output

192.168.1.2 (tcp/445)

```
Here is a list of office files which have been found on the remote SMB
shares :

  + C$ :

    - \Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.14393.0_none_4594460740901c48\MsoIrmProtector.doc
    - \Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.14393.0_none_3b3f9bb50c2f5a4d\MsoIrmProtector.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RUGCO6S.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RSU2DGT.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RHU0278.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RDNH2XB.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$R824VH9.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$R60G5H3.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IHU0278.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IDNH2XB.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$I824VH9.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$I60G5H3.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$I16XEC7.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$ISU2DGT.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IUGCO6S.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IV12NDR.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IV2QP67.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$IW61KRL.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$R16XEC7.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RV12NDR.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RV2QP67.doc
    - \$Recycle.Bin\S-1-5-21-2552265371-3243985514-2585313438-1001\$RW61KRL.doc
```

```
      - \Windows\System32\MSDRM\MsoIrmProtector.doc
      - \Windows\SysWOW64\M [...]
```

27524 (1) - Microsoft Office Detection

Synopsis

The remote Windows host contains an office suite.

Description

Microsoft Office is installed on the remote host.

See Also

https://products.office.com/en-US/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/10/23, Modified: 2018/03/13

Plugin Output

192.168.1.2 (tcp/0)

```
The remote host has the following Microsoft Office 2010 Service Pack 2 components installed :

  - Word : 14.0.7182.5000
  - Excel : 14.0.7183.5000
  - PowerPoint : 14.0.7176.5000
```

28211 (1) - Flash Player Detection

Synopsis

The remote Windows host contains a browser enhancement for displaying multimedia content.

Description

There is at least one instance of Adobe Flash Player installed on the remote Windows host.

See Also

http://www.adobe.com/products/flashplayer/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/11/14, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
Nessus found the following instances of Flash Player installed on the
remote host :

  - ActiveX control (for Internet Explorer) :
    C:\Windows\System32\Macromed\Flash\Flash.ocx, 26.0.0.137
```

34196 (1) - Google Chrome Detection (Windows)

Synopsis

The remote Windows host contains a web browser.

Description

Google Chrome, a web browser from Google, is installed on the remote Windows host.

See Also

http://www.google.com/chrome

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2008/09/12, Modified: 2015/10/13

Plugin Output

192.168.1.2 (tcp/445)

```
The following instance of Google Chrome is installed on the remote
host :

  Path              : C:\Program Files (x86)\Google\Chrome\Application
  Installed version : 60.0.3112.113

Note that Nessus only looked in the registry for evidence of Google
Chrome. If there are multiple users on this host, you may wish to
enable the 'Perform thorough tests' setting and re-scan. This will
cause Nessus to scan each local user's directory for installs.
```

38153 (1) - Microsoft Windows Summary of Missing Patches

Synopsis

The remote host is missing several Microsoft security patches.

Description

This plugin summarizes updates for Microsoft Security Bulletins or Knowledge Base (KB) security updates that have not been installed on the remote Windows host based on the results of either a credentialed check using the supplied credentials or a check done using a supported third-party patch management tool.

Review the summary and apply any missing updates in order to be up to date.

Solution

Run Windows Update on the remote host or use a patch management solution.

Risk Factor

None

Plugin Information:

Published: 2009/04/24, Modified: 2017/05/25

Plugin Output

192.168.1.2 (tcp/445)

```
The patches for the following bulletins or KBs are missing on the remote host :

 - MS15-124 ( http://technet.microsoft.com/en-us/security/bulletin/ms15-124 )
 - MS16-087 ( http://technet.microsoft.com/en-us/security/bulletin/ms16-087 )
 - KB4015217 ( https://support.microsoft.com/en-us/help/4015217 )
 - KB4019472 ( https://support.microsoft.com/en-us/help/4019472 )
 - KB4022715 ( https://support.microsoft.com/en-us/help/4022715 )
 - KB4034658 ( https://support.microsoft.com/en-us/help/4034658 )
 - KB4034662 ( https://support.microsoft.com/en-us/help/4034662 )
 - KB3128027 ( https://support.microsoft.com/en-us/help/3128027 )
 - KB3141537 ( https://support.microsoft.com/en-us/help/3141537 )
 - KB4011061 ( https://support.microsoft.com/en-us/help/4011061 )
 - KB4038782 ( https://support.microsoft.com/en-us/help/4038782 )
 - KB4038806 ( https://support.microsoft.com/en-us/help/4038806 )
 - KB3213630 ( https://support.microsoft.com/en-us/help/3213630 )
 - KB4011196 ( https://support.microsoft.com/en-us/help/4011196 )
 - KB4041691 ( https://support.microsoft.com/en-us/help/4041691 )
 - KB4049179 ( https://support.microsoft.com/en-us/help/4049179 )
 - KB4011197 ( https://support.microsoft.com/en-us/help/4011197 )
 - KB4011270 ( https://support.microsoft.com/en-us/help/4011270 )
 - KB4048951 ( https://support.microsoft.com/en-us/help/4048951 )
 - KB4048953 ( https://support.microsoft.com/en-us/help/4048953 )
 - KB4011614 ( https://support.microsoft.com/en-us/help/4011614 )
 - KB4053577 ( https://support.microsoft.com/en-us/help/4053577 )
 - KB4053579 ( https://support.microsoft.com/en-us/help/4053579 )
 - KB4011273 ( https://support.microsoft.com/en-us/help/4011273 )
 - KB4011659 ( https://support.microsoft.com/en-us/help/4011659 )
```

```
  - KB4011660 ( https://support.microsoft.com/en-us/help/4011660 )
  - KB4056887 ( https://support.microsoft.com/en-us/help/4056887 )
  - KB4056890 ( https://support.microsoft.com/en-us/help/4056890 )
  - KB4057142 ( https://support.microsoft.com/en-us/help/4057142 )
  - KB4011711 ( https://support [...]
```

38689 (1) - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.

See Also

https://support.microsoft.com/en-us/kb/260324

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/05/05, Modified: 2017/01/26

Plugin Output

192.168.1.2 (tcp/445)

```
Last Successful logon : kamata
```

42898 (1) - SMB Registry : Stop the Registry Service after the scan (WMI)

Synopsis

The registry service was stopped after the scan.

Description

To perform a full credentialed scan, Nessus needs the ability to connect to the remote registry service (RemoteRegistry). If the service is down and if Nessus automatically enabled the registry for the duration of the scan, this plugins will stop it afterwards.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/11/25, Modified: 2018/02/06

Plugin Output

192.168.1.2 (tcp/0)

```
The registry service was successfully stopped after the scan.
```

44401 (1) - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

Plugin Information:

Published: 2010/02/05, Modified: 2017/06/14

Plugin Output

192.168.1.2 (tcp/445)

```
The following services are set to start automatically :

  AVP startup parameters :
    Display name : Kaspersky Endpoint Security Service
    Service name : AVP
    Log on as : LocalSystem
    Executable path : "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for
 Windows SP1\avp.exe" -r
    Dependencies : cryptSvc/

  AudioEndpointBuilder startup parameters :
    Display name : Windows Audio Endpoint Builder
    Service name : AudioEndpointBuilder
    Log on as : LocalSystem
    Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

  Audiosrv startup parameters :
    Display name : Windows Audio
    Service name : Audiosrv
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
    Dependencies : AudioEndpointBuilder/RpcSs/

  BFE startup parameters :
    Display name : Base Filtering Engine
    Service name : BFE
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
    Dependencies : RpcSs/
```

```
 BITS startup parameters :
   Display name : Background Intelligent Transfer Service
   Service name : BITS
   Log on as : LocalSystem
   Executable path : C:\Windows\System32\svchost.exe -k netsvcs
   Dependencies : RpcSs/

 CDPSvc startup parameters :
   Display name : Connected Devices Platform Service
   Service name : CDPSvc
   Log on as : NT AUTHORITY\LocalService
   Executable path : C:\Windows\system32\svchost.exe -k LocalService

 CDPUserSvc_74d7364 startup parameters :
   Display name : CDPUserSvc_74d7364
   Service name : CDPUserSvc_74d7364
   Executable path : C:\Windows\system32\svchost.exe -k UnistackSvcGroup

 CryptSvc startup parameters :
   Display name : Cryptographic Services
   Service name : CryptSvc
   Log on as : NT Authority\NetworkService
   Executable path : C:\Windows\system32\svchost.exe -k NetworkService
   Dependencies : RpcSs/

 Dhcp startup parameters :
   Display name : DHCP Client
[...]
```

48942 (1) - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/31, Modified: 2018/03/09

Plugin Output

192.168.1.2 (tcp/445)

```
Operating system version = 10.14393
Architecture = x64
Build lab extended = 14393.1480.amd64fre.rs1_release.170706-2004
```

50346 (1) - Microsoft Update Installed

Synopsis

A software updating service is installed.

Description

Microsoft Update, an expanded version of Windows Update, is installed on the remote Windows host. This service provides updates for the operating system and Internet Explorer as well as other Windows software such as Microsoft Office, Exchange, and SQL Server.

See Also

http://update.microsoft.com/microsoftupdate/v6/default.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/10/26, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

51351 (1) - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net/

http://www.nessus.org/u?af642f11

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/12/20, Modified: 2017/12/11

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host has the following version(s) of Microsoft .NET Framework
installed :

 + Version : 2.0.50727
 - Full Version : 2.0.50727.4927
 - SP : 2

 + Version : 3.0
 - Full Version : 3.0.30729.4926
 - SP : 2

 + Version : 3.5
 - Full Version : 3.5.30729.4926
 - SP : 1
 - Path : C:\Windows\Microsoft.NET\Framework64\v3.5\

 + Version : 4.7
 - Install Type : Full
 - Full Version : 4.7.02053
 - Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
```

```
  + Version : 4.7
  - Install Type : Client
  - Full Version : 4.7.02053
  - Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
```

52715 (1) - TeamViewer Version Detection

Synopsis

A remote control service is installed on the remote Windows host.

Description

TeamViewer, a remote control service, is installed on the remote Windows host.

See Also

https://www.teamviewer.com/en/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/03/18, Modified: 2018/02/07

Plugin Output

192.168.1.2 (tcp/0)

```
Path    : C:\Program Files (x86)\TeamViewer
Version : 10.0.47484
```

57033 (1) - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates.

Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/06, Modified: 2016/02/12

Plugin Output

192.168.1.2 (tcp/445)

```
Nessus is able to test for missing patches using :
  Nessus
```

58181 (1) - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/03/01, Modified: 2015/03/17

Plugin Output

192.168.1.2 (tcp/445)

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {bd73f518-30d3-46a6-adae-f580bf66fa43}
Network Connection : ......
NameServer: 192.168.1.1
```

58452 (1) - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi on\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2012/03/23, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
The following startup item was found :

  AVP - C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\avp.exe
  HotKeysCmds - C:\Windows\system32\hkcmd.exe
  IgfxTray - C:\Windows\system32\igfxtray.exe
  Persistence - C:\Windows\system32\igfxpers.exe
  SynLenovoHelper - %ProgramFiles%\Synaptics\SynTP\SynLenovoHelper.exe
  SynTPEnh - %ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
```

60119 (1) - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx

https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/07/25, Modified: 2017/12/15

Plugin Output

192.168.1.2 (tcp/445)

```
Share path : \\HOST-M05\scan
Local path : C:\scan
[*] Allow ACE for BUILTIN\Administrators: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\HOST-M05\Users
Local path : C:\Users
[*] Allow ACE for BUILTIN\Administrators: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
```

```
    FILE_GENERIC_EXECUTE:      YES
```

62042 (1) - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/09/11, Modified: 2013/03/28

Plugin Output

192.168.1.2 (tcp/0)

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB3186568, Installed on: 2017/07/13
KB4013418, Installed on: 2017/04/03
KB4023834, Installed on: 2017/06/14
KB4025339, Installed on: 2017/08/01
KB4025376, Installed on: 2017/08/01
```

63080 (1) - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?3eee2c7c

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2012/11/28, Modified: 2012/11/28

Plugin Output

192.168.1.2 (tcp/445)

```
  Name     : \dosdevices\e:
  Data     : _??_USBSTOR#Disk&Ven_GH&Prod_USB2.0_Memory&Rev_PMAP#070748A4EC1F3808&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5f003f003f005f005500530042005300540 04f00520023004400690073006b002600560065006e005f00470048002600500072006f0064005

  Name     : \??\volume{73bc080e-20ce-11e7-8161-002315ce6dbc}
  Data     : _??_USBSTOR#Disk&Ven_TOSHIBA&Prod_TransMemory-
Mx&Rev_PMAP#60A44C429E4CE11130021D3B&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5f003f003f005f005500530042005300540 04f00520023004400690073006b002600560065006e005f0054004f00530048004900420041002

  Name     : \??\volume{22446332-265d-11e7-8164-f0def13b5498}
  Data     : \??\USBSTOR#CdRom&Ven_MATSHITA&Prod_BD-
MLT_UJ260AF&Rev_1.20#0010101D4012134F&0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c005500530042005300540 04f00520023004300640052006f006d002600560065006e005f004d0041005400530048004900 5

  Name     : \dosdevices\d:
  Data     : )P
  Raw data : 29f001d [...]
```

66334 (1) - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Published: 2013/07/08, Modified: 2018/03/29

Plugin Output

192.168.1.2 (tcp/0)

```
. You need to take the following 9 actions :

+ Install the following Microsoft patches :
- KB4088787 (12 vulnerabilities)
- KB4011711 (3 vulnerabilities)
- KB4011675 (4 vulnerabilities)
- KB4011674 (5 vulnerabilities)
- KB3141537 (1 vulnerabilities)
- KB3128027 (1 vulnerabilities)
- KB3125869

[ Adobe Flash Player <= 28.0.0.161 (APSB18-05) (108281) ]

+ Action to take : Upgrade to Adobe Flash Player version 29.0.0.113 or later.

+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).


[ Google Chrome < 65.0.3325.146 Multiple Vulnerabilities (107220) ]

+ Action to take : Upgrade to Google Chrome version 65.0.3325.146 or later.

+Impact : Taking this action will resolve 80 different vulnerabilities (CVEs).
```

66350 (1) - Microsoft Windows Wireless Network History

Synopsis

This plugin identifies wireless networks that the computer has connected to.

Description

Using the supplied credentials, this plugin reports wireless networks that this computer has connected to as well as the settings for Windows Vista and later systems.

See Also

http://www.nessus.org/u?7a21f7c2

Solution

Make sure that use of the reported networks agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2013/05/08, Modified: 2015/01/12

Plugin Output

192.168.1.2 (tcp/445)

```
SSID : L01G_EAFC4DC3_A
Managed : FALSE
Description : L01G_EAFC4DC3_A
GUID : {439830EA-A016-4614-A036-36CD362BBB3A}
DateCreated : Thursday, 07/13/2017 01:26:10.634 PM
DateLastConnected : Tuesday, 08/01/2017 07:42:37.695 AM
Description : L01G_EAFC4DC3_A
DefaultGatewayMac : 583f54bfe5eb
DnsSuffix : <jW>
FirstNetwork : L01G_EAFC4DC3_A
Source : 8
Category : 0
Security Settings are not logged on the system.

SSID : FON_FREE_INTERNET
Managed : FALSE
Description : FON_FREE_INTERNET
GUID : {24A909E0-331F-48FE-A75D-4E8FA1BB522C}
DateCreated : Friday, 04/14/2017 04:37:33.99 PM
DateLastConnected : Thursday, 05/04/2017 10:09:54.883 AM
Description : FON_FREE_INTERNET
DefaultGatewayMac : 0018843c99c9
DnsSuffix : lan
```

```
FirstNetwork : FON_FREE_INTERNET
Source : 8
Category : 0
Security Settings are not logged on the system.

SSID : FON_FREE_INTERNET  2
Managed : FALSE
Description : FON_FREE_INTERNET  2
GUID : {CE9B885F-5E1E-497C-97BE-95A892EF3BB6}
DateCreated : Wednesday, 11/22/2017 03:46:35.267 PM
DateLastConnected : Wednesday, 11/22/2017 05:55:46.539 PM
Description : FON_FREE_INTERNET  2
DefaultGatewayMac : 001884380f89
DnsSuffix : lan
FirstNetwork : FON_FREE_INTERNET  2
Source : 8
Category : 0
Security Settings are not logged on the system.

SSID : DIRECT-ERNETPRO-M05UUPY
Managed : FALSE
Description : DIRECT-ERNETPRO-M05UUPY
GUID : {0410E6B1-C8EA-4742-9EC0-72C7D4469129}
DateCreated : Thursday, 05/04/2017 06:32:00.850 PM
DateLastConnected : Thursday, 05/04/2017 06:32:00.853 PM
Description : DIRECT-ERNETPRO-M05UUPY
DefaultGatewayMac : 4e554c4c
DnsSuffix : <jW>
FirstNetwork : DIRECT-ERNETPRO-M05UUPY
Source : 2048
Category : 0
Security Settings are not logged on the system.
```

66424 (1) - Microsoft Malicious Software Removal Tool Installed

Synopsis

An antimalware application is installed on the remote Windows host.

Description

The Microsoft Malicious Software Removal Tool is installed on the remote host. This tool is an application that attempts to detect and remove known malware from Windows systems.

See Also

http://www.microsoft.com/security/pc-security/malware-removal.aspx

http://support.microsoft.com/kb/891716

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/05/15, Modified: 2017/05/10

Plugin Output

192.168.1.2 (tcp/445)

```
File                : C:\Windows\system32\MRT.exe
Version             : 5.50.14000.0
Release at last run : unknown
Report infection information to Microsoft : Yes
```

72367 (1) - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

http://windows.microsoft.com/en-us/internet-explorer/download-ie

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2014/02/06, Modified: 2014/02/13

Plugin Output

192.168.1.2 (tcp/445)

```
Version  : 11.1480.14393.0
```

77605 (1) - Microsoft OneNote Detection

Synopsis

The remote Windows host contains Microsoft OneNote.

Description

Microsoft OneNote is installed on the remote host.

See Also

http://www.onenote.com/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2014/09/10, Modified: 2018/04/03

Plugin Output

192.168.1.2 (tcp/0)

```
Path    : C:\Program Files (x86)\Microsoft Office\Office14\OneNote.exe
Version : 14.0.7162.5000
```

77668 (1) - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot%\prefetch*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?0ab4c9af

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2014/09/12, Modified: 2014/09/12

Plugin Output

192.168.1.2 (tcp/0)

```
+ HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3

+ Prefetch file list :
  - \Windows\prefetch\60.0.3112.113_60.0.3112.101_C-206DFAF2.pf
  - \Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf
  - \Windows\prefetch\AUDIODG.EXE-BDFD3029.pf
  - \Windows\prefetch\AVP.EXE-218ED2DD.pf
  - \Windows\prefetch\B2.EXE-9112FF47.pf
  - \Windows\prefetch\B2SETUP.EXE-E32D32C9.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-38A6ADBA.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-61059E6B.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-E8F29D24.pf
  - \Windows\prefetch\BATCHINSTALLER.EXE-F037BB8F.pf
  - \Windows\prefetch\BK27300J.EXE-4FB98F76.pf
  - \Windows\prefetch\BROWSER_BROKER.EXE-E6357BB0.pf
  - \Windows\prefetch\BYTECODEGENERATOR.EXE-292CE66A.pf
  - \Windows\prefetch\BYTECODEGENERATOR.EXE-C1E9BCE6.pf
  - \Windows\prefetch\CHANGEPK.EXE-156CA255.pf
```

```
- \Windows\prefetch\CHROME.EXE-D999B1BA.pf
- \Windows\prefetch\CHROME.EXE-D999B1BB.pf
- \Windows\prefetch\CHROME.EXE-D999B1BC.pf
- \Windows\prefetch\CHROME.EXE-D999B1C0.pf
- \Windows\prefetch\CHROME.EXE-D999B1C1.pf
- \Windows\prefetch\CHROME.EXE-D999B1C2.pf
- \Windows\prefetch\CMD.EXE-4A81B364.pf
- \Windows\prefetch\COMPATTELRUNNER.EXE-DB97728F.pf
- \Windows\prefetch\CONHOST.EXE-1F3E9D7E.pf
- \Windows\prefetch\CONSENT.EXE-531BD9EA.pf
- \Windows\prefetch\CREDENTIALUIBROKER.EXE-2FE21806.pf
- \Windows\prefetch\CSC.EXE-A3B8D95D.pf
- \Windows\prefetch\CSRSS.EXE-3FE41F7E.pf
- \Windows\prefetch\CVTRES.EXE-069169FB.pf
- \Windows\prefetch\DASHOST.EXE-5E5F38F6.pf
- \Windows\prefetch\DATAEXCHANGEHOST.EXE-BE987727.pf
- \Windows\prefetch\DEFRAG.EXE-588F90AD.pf
- \Windows\prefetch\DISM.EXE-DE199F71.pf
- \Windows\prefetch\DLLHOST.EXE-2CE79F17.pf
- \Windows\prefetch\DLLHOST.EXE-46FA2603.pf
- \Windows\prefetch\DLLHOST.EXE-570206E5.pf
- \Windows\prefetch\DLLHOST.EXE-5E46FA0D.pf
- \Windows\prefetch\DLLHOST.EXE-6BCB9FAA.pf
- \Windows\prefetch\DLLHOST.EXE-766398D2.pf
-  [...]
```

90511 (1) - MS KB3152550: Update to Improve Wireless Mouse Input Filtering

Synopsis

The remote Windows host is missing an update to wireless mouse input filtering.

Description

The remote Windows host is missing an update to the wireless mouse input filtering functionality. The missing update enhances security by filtering out QWERTY key packets in keystroke communications issued when receiving communication from USB wireless dongles. The update resolves a vulnerability that allows a local attacker in the physical proximity of the wireless mouse range to inject keyboard HID packets into Microsoft wireless mouse devices through the use of USB dongles.

See Also

https://technet.microsoft.com/en-us/library/security/3152550

Solution

Microsoft has released a set of patches for Windows 7, 8.1, and 10.

Risk Factor

None

References

MSKB	3152550

Plugin Information:

Published: 2016/04/13, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
Nessus has determined that the remote Windows host is missing files
that are created upon installation of the update corresponding to
Microsoft Security Advisory 3152550.
```

92364 (1) - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2018/02/09

Plugin Output

192.168.1.2 (tcp/0)

```
Environment variable information attached.
```

92365 (1) - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
Windows hosts file attached.
```

92367 (1) - Microsoft Windows PowerShell Execution Policy

Synopsis

Nessus was able to collect and report the PowerShell execution policy for the remote host.

Description

Nessus was able to collect and report the PowerShell execution policy for the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy : Restricted
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy :
 Restricted
```

92421 (1) - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141

Internet Explorer typed URL report attached.
```

92424 (1) - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
@%systemroot%\system32\themeservice.dll,-8192 : Themes
@%systemroot%\system32\mprmsg.dll,-32011 : Remote Access IP ARP Driver
@%systemroot%\system32\tabsvc.dll,-100 : Touch Keyboard and Handwriting Panel Service
@%systemroot%\system32\bfe.dll,-1002 : ... ..... .... (BFE) o.........h....... ..... ......
 (IPsec) .......W..... ... ...........Y.....gY.BFE .....
\b~_o!.kY.h.....n......L'EkN.Y.hqk.IPsec ..h........ ........n.,\r.j.\n..hj.~Y.
c:\windows\system32,@elscore.dll,-8 : Microsoft Transliteration .......WK.....W
@%systemroot%\system32\browser.dll,-101 : ......\nn.......n
```

92425 (1) - Microsoft Office File History

Synopsis

Nessus was able to enumerate files opened in Microsoft Office on the remote host.

Description

Nessus was able to gather evidence of files that were opened using any Microsoft Office application. The report was extracted from Office MRU (Most Recently Used) registry keys.

See Also

https://products.office.com/en-US/

http://www.taksati.org/mru/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\2012.LNK
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\3067.......;...n. .LNK
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\3115..... O .LNK
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\index.dat
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\.........Q.B.... .LNK
C:\\Users\haruka\AppData\Roaming\Microsoft\Office\Recent\.P.
```

92431 (1) - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
Administrator
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\Administrator\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\Administrator\AppData\Roaming\Microsoft
\Windows\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\Administrator\Downloads
  - recent : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\Administrator\Videos
  - my music : C:\Users\Administrator\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\Administrator\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\Administrator\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\Administrator\AppData\LocalLow
  - sendto : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\Administrator\Documents
  - administrative tools : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu
\Programs\Administrative Tools
  - startup : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - history : C:\Users\Administrator\AppData\Local\Microsoft\Windows\History
  - nethood : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\Administrator\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\Administrator\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function instead
  - local appdata : C:\Users\Administrator\AppData\Local
  - my pictures : C:\Users\Administrator\Pictures
  - templates : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\Administra [...]
```

92434 (1) - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/07/19, Modified: 2017/08/30

Plugin Output

192.168.1.2 (tcp/0)

```
C:\\Users\Administrator\Downloads\desktop.ini
C:\\Users\haruka\Downloads\2017.05.13.zip
C:\\Users\haruka\Downloads\2017.5.1.zip
C:\\Users\haruka\Downloads\2017.5.14.16 (1).zip
C:\\Users\haruka\Downloads\2017.5.14.16.zip
C:\\Users\haruka\Downloads\2017.5.9:h.s.p.zip
C:\\Users\haruka\Downloads\20170508113527.pdf
C:\\Users\haruka\Downloads\20170508113558.pdf
C:\\Users\haruka\Downloads\20170508113641.pdf
C:\\Users\haruka\Downloads\20170508113708.pdf
C:\\Users\haruka\Downloads\20170508113721.pdf
C:\\Users\haruka\Downloads\20170508113748.pdf
C:\\Users\haruka\Downloads\20170508113827.pdf
C:\\Users\haruka\Downloads\20170508113909.pdf
C:\\Users\haruka\Downloads\20170508113951.pdf
C:\\Users\haruka\Downloads\20170508114024.pdf
C:\\Users\haruka\Downloads\20170508114123.pdf
C:\\Users\haruka\Downloads\20170508114208.pdf
C:\\Users\haruka\Downloads\20170508114237.pdf
C:\\Users\haruka\Downloads\20170508114334.pdf
C:\\Users\haruka\Downloads\20170508114408.pdf
C:\\Users\haruka\Downloads\20170508114430.pdf
C:\\Users\haruka\Downloads\20170508114508.pdf
C:\\Users\haruka\Downloads\20170508114603.pdf
C:\\Users\haruka\Downloads\20170508114619.pdf
C:\\Users\haruka\Downloads\20170508114639.pdf
C:\\Users\haruka\Downloads\20170508114659.pdf
C:\\Users\haruka\Downloads\20170508120447.pdf
C:\\Users\haruka\Downloads\20170508120500.pdf
C:\\Users\haruka\Downloads\20170508120512.pdf
C:\\Users\haruka\Downloads\20170508120521.pdf
```

```
C:\\Users\haruka\Downloads\20170508120530.pdf
C:\\Users\haruka\Downloads\20170508120537.pdf
C:\\Users\haruka\Downloads\20170508120544.pdf
C:\\Users\haruka\Downloads\20170508120554.pdf
C:\\Users\haruka\Downloads\20170508120602.pdf
C:\\Users\haruka\Downloads\20170508120611.pdf
C:\\Users\haruka\Downloads\20170508120622.pdf
C:\\Users\haruka\Downloads\20170508120631.pdf
C:\\Users\haruka\Downloads\20170508120641.pdf
C:\\Users\haruka\Downloads\20170508120650.pdf
C:\\Users\haruka\Downloads\20170508120700.pdf
C:\\Users\haruka\Downloads\20170508120711.pdf
C:\\Users\haruka\Downloads\20170508120720.pdf
C:\\Users\haruka\Downloads\20170508 [...]
```

93232 (1) - Microsoft Office Compatibility Pack Installed (credentialed check)

Synopsis

A compatibility application is installed on the remote host.

Description

Microsoft Office Compatibility Pack, used to enable older versions of Microsoft Office applications to view and edit files created with newer versions of Microsoft Office applications, is installed on the remote Windows host.

See Also

https://support.microsoft.com/en-us/kb/923505

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/08/30, Modified: 2018/04/03

Plugin Output

192.168.1.2 (tcp/445)

```
Office Compatibility Pack is installed with the following components:

  Component : Excel Converter
  Version   : 14.0.7183.5000
  Path      : C:\Program Files (x86)\Microsoft Office\Office14\Excelcnv.exe

  Component : Word Converter
  Version   : 14.0.4762.1000
  Path      : C:\Program Files (x86)\Microsoft Office\Office14\Wordconv.exe
```

93962 (1) - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2016/10/11, Modified: 2018/03/30

Plugin Output

192.168.1.2 (tcp/445)

```
Cumulative Rollup : 07_2017 [KB4025339]

Latest effective update level : 07_2017
File checked                  : C:\Windows\System32\shell32.dll
File version                  : 10.0.14393.1478
Associated KB                 : 4025339
```

96533 (1) - Chrome Browser Extension Enumeration

Synopsis

One or more Chrome browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Chrome browser extensions installed on the remote host.

See Also

https://chrome.google.com/webstore/category/extensions

Solution

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2017/01/16, Modified: 2018/03/29

Plugin Output

192.168.1.2 (tcp/445)

```
User : haruka
|- Browser : Chrome
  |- Add-on information :

    Name        : Google Slides
    Description : Create and edit presentations
    Version     : 0.9
    Update Date : May.  4, 2017 at 09:02:10 GMT
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\aapocclcgogkmnckokdopfmhonfmgoek\0.9_0

    Name        : Google Docs
    Description : Create and edit documents
    Version     : 0.9
    Update Date : May.  4, 2017 at 09:02:12 GMT
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\aohghmighlieiainnegkcijnfilokake\0.9_0

    Name        : Google Drive
    Description : Google Drive: create, share and keep all your stuff in one place.
    Version     : 14.1
    Update Date : May.  4, 2017 at 09:02:16 GMT
```

```
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\apdfllckaahabafndbhieahigkjlhalf\14.1_0

    Name        : YouTube
    Version     : 4.2.8
    Update Date : May.  4, 2017 at 09:02:17 GMT
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.8_0

    Name        : Google Sheets
    Description : Create and edit spreadsheets
    Version     : 1.1
    Update Date : May.  4, 2017 at 09:02:20 GMT
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\felcaaldnbdncclmgdcncolpebgiejap\1.1_0

    Name        : Google Docs Offline
    Description : Get things done offline with the Google Docs family of products.
    Version     : 1.4
    Update Date : May.  4, 2017 at 09:18:53 GMT
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.4_2

    Name        : Chrome Web Store Payments
    Description : Chrome Web Store Payments
    Version     : 1.0.0.2
    Path        : C:\Users\haruka\AppData\Local\Google\Chrome\User Data\Default\Extensions
\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.2_0

    Name        : Gmail
    D [...]
```

97086 (1) - Server Message Block (SMB) Protocol Version 1 Enabled

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/09, Modified: 2017/10/26

Plugin Output

192.168.1.2 (tcp/445)

```
SMBv1 server is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : NULL or missing
SMB1protocol feature is enabled based on the following key :
```

```
    - HKLM\SYSTEM\CurrentControlSet\Services\srv
  SMBv1 client is enabled :
    - HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10\Start : 2
```

100871 (1) - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

103871 (1) - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2017/10/17, Modified: 2017/10/17

Plugin Output

192.168.1.2 (tcp/445)

```
Network Adapter Driver Description : Intel(R) 82577LM Gigabit Network Connection
Network Adapter Driver Version     : 12.15.22.6

Network Adapter Driver Description : Intel(R) Centrino(R) Advanced-N 6250 AGN Driver
Network Adapter Driver Version     : 15.12.0.8
```

106716 (1) - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

192.168.1.2 (tcp/445)

```
The remote host supports the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.1        Windows 10
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 14% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Google Chrome < 65.0.3325.146 Multiple Vulnerabilities: Upgrade to Google Chrome version 65.0.3325.146 or later.	80	1
Adobe Flash Player <= 28.0.0.161 (APSB18-05): Upgrade to Adobe Flash Player version 29.0.0.113 or later.	16	1
Install KB4088787	12	1
Install KB4011674	5	1
Install KB4011675	4	1
Install KB4011711	3	1
Install KB3141537	1	1
Install KB3128027	1	1