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意をお願いいたします。

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	192.168.0.82
2	192.168.0.84
3	192.168.0.90
4	192.168.0.251
5	192.168.0.253..
6	192.168.0.254

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。

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できます。今回のプラットフォーム脆弱性診断ではCVE以外の脆弱性リストも参照して診断しています。

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、個々の脆弱性については「SEVERITY」として重要度を判別しています。

■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)を順番に評価していくことで、脆弱性の深刻度を0(低)～10.0(高)の数値で表します。

■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	1
HIGH	2
MEDIUM	25
LOW	6

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くることから、設定等を変更してこのような情報が漏洩しない適切な対策が必要です。

SEVERITY	CVSS	NAME
CRITICAL	10	実行可能ファイルへの壊れたリンクを持つLinuxデーモン
HIGH	7.5	Microsoft Windows SMBは権限のないアクセスを共有
MEDIUM	6.4	SSL証明書を信頼できない
MEDIUM	6.4	SSL自己署名証明書
MEDIUM	5.1	Microsoft WindowsリモートデスクトッププロトコルサーバーMan-in-the-Middle弱点
MEDIUM	5	SSL証明書有効期限
MEDIUM	5	弱いハッシュアルゴリズムを使用して署名されたSSL証明書
MEDIUM	5	SMB署名が無効
MEDIUM	5	SSL中強度暗号スイートサポート
MEDIUM	5	弱いハッシュアルゴリズムを使用して署名されたSSL証明書
MEDIUM	5	間違ったホスト名のSSL証明書
MEDIUM	4.3	ターミナルサービスの暗号化レベルが中または低
MEDIUM	4.3	ターミナルサービスはネットワークレベル認証（NLA）のみを使用しません
MEDIUM	4.3	サポートされている弱いSSHアルゴリズム
LOW	2.6	ターミナルサービスの暗号化レベルはFIPS-140準拠ではありません
LOW	2.6	SSHサーバCBCモード暗号が有効
LOW	2.6	SSH弱いMACアルゴリズムが有効
LOW	2.1	パッケージシステムによって管理されていないネットワークデーモン
LOW	N/A	SSL証明書チェーンには2048ビット未満のRSAキーが含まれています

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UNIX系OSの常駐プログラムに対応する実行可能ファイルへのリンクが壊れている不具合が見つかりました。攻撃者が悪質な活動を隠そうとしてファイルを削除した結果のから生じる不具合の可能性もあるため早急に確認してください。

【Microsoft Windows SMBに関する脆弱性】
1つ以上のWindows共有があり、指定された場所でネットワーク経由でアクセスできる状態になっています。攻撃者が機密データを読み書きする可能性がありますので状況を確認し、不必要であればアクセスを制限してください。

▽攻撃者によるリモート制御の恐れ▽
Windowsネットワークにおけるファイル共有プロトコルのSMBですが設定を間違えるとリモートでコードが実行される可能性があります。

【SSLに関する脆弱性が多く検出されました】
インターネット上でデータを暗号化して送受信する仕組み（プロトコル）であるSSL（Secure Sockets Layer）に多くの不具合が検出されました。「サーバ証明書の有効期限切れ」などは直ちに深刻なインシデントを引き起こすものではありませんがサーバに接続するユーザーへの不信感にも繋がりますので一度、見直すことをお勧めします。全脆弱性34件中、14件含まれていました。

Port Scan Sample

CyberSecurityReport

Tue, 03 Apr 2018 20:23:46 JST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

44657 (1) - Linux Daemons with Broken Links to Executables

Synopsis

A daemon on the remote Linux host may need to be restarted.

Description

By examining the '/proc' filesystem on the remote Linux host, Nessus has identified at least one currently-running daemon for which the link to the corresponding executable is broken.

This can occur when the executable associated with a daemon is replaced on disk but the daemon itself has not been restarted. And if the changes are security-related, the system may remain vulnerable to attack until the daemon is restarted.

Alternatively, it could result from an attacker removing files in an effort to hide malicious activity.

Solution

Inspect each reported daemon to determine why the link to the executable is broken.

Risk Factor

Critical

CVSS Base Score

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

Plugin Information:

Published: 2010/02/17, Modified: 2015/10/21

Plugin Output

192.168.0.90 (tcp/0)

```
The following daemons are associated with broken links to
executables :

  - 68 udp: (/usr/sbin/dhclient;5ac35977)
  - 37021 udp: (/usr/sbin/dhclient;5ac35977)
  - 3839 udp: (/usr/sbin/dhclient;5ac35977)
```

42411 (2) - Microsoft Windows SMB Shares Unprivileged 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

High

CVSS Base Score

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

CVSS Temporal Score

7.5 (CVSS2#E:H/RL:U/RC:ND)

References

BID	8026
CVE	CVE-1999-0519
CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Published: 2009/11/06, Modified: 2011/03/27

Plugin Output

192.168.0.84 (tcp/445)

```
The following shares can be accessed as kamata :

- Users  - (readable)
```

```
  + Content of this share :
..
Default
desktop.ini
kamata.HOST
Packages
```

192.168.0.253 (tcp/445)

```
The following shares can be accessed as kamata :

- yaccbackup$  - (readable,writable)
  + Content of this share :
..
_KD11_*..>.....,14...,15.(14.^15.).zbk

- Users  - (readable)
  + Content of this share :
..
Default
Default.migrated
desktop.ini
kamata.HOST
kamata.HOST.000
```

51192 (5) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

192.168.0.82 (tcp/3389)

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject  :  CN=HOST-M09.HOST.co.jp  |-
Issuer  : CN=HOST-M09.HOST.co.jp
```

192.168.0.84 (tcp/3389)

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject  :  CN=HOST-M08.HOST.co.jp  |-
Issuer  : CN=HOST-M08.HOST.co.jp
```

192.168.0.90 (tcp/8834)

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=localhost.localdomain
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

192.168.0.251 (tcp/443)

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=TS Series NAS
|-Not After : Aug 21 06:50:42 2012 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=TS Series NAS
|-Issuer  : C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=TS Series NAS
```

192.168.0.254 (tcp/443)

```
The following certificate was at the top of the certificate
```

```
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/
E=support@fortinet.com
|-Issuer  : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/
E=support@fortinet.com
```

45411 (4) - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

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 Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

192.168.0.82 (tcp/3389)

```
The identities known by Nessus are :

  192.168.0.82
  192.168.0.82

The Common Name in the certificate is :

HOST-M09.HOST.co.jp
```

192.168.0.84 (tcp/3389)

```
The identities known by Nessus are :

  192.168.0.84
  192.168.0.84
```

```
The Common Name in the certificate is :

HOST-M08.HOST.co.jp
```

192.168.0.251 (tcp/443)

```
The identities known by Nessus are :

  192.168.0.251
  192.168.0.251

The Common Name in the certificate is :

  TS Series NAS
```

192.168.0.253 (tcp/3389)

```
The identities known by Nessus are :

  192.168.0.253
  192.168.0.253

The Common Name in the certificate is :

SRV-WIN7.HOST.co.jp
```

57582 (4) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

192.168.0.82 (tcp/3389)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=HOST-M09.HOST.co.jp
```

192.168.0.84 (tcp/3389)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=HOST-M08.HOST.co.jp
```

192.168.0.251 (tcp/443)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=TS Series NAS
```

192.168.0.254 (tcp/443)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/
E=support@fortinet.com
```

57608 (4) - SMB Signing Disabled

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

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)

Plugin Information:

Published: 2012/01/19, Modified: 2016/12/09

Plugin Output

192.168.0.82 (tcp/445)
192.168.0.84 (tcp/445)
192.168.0.251 (tcp/445)
192.168.0.253 (tcp/445)

35291 (2) - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108

XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Published: 2009/01/05, Modified: 2018/02/20

Plugin Output

192.168.0.251 (tcp/443)

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=TS Series NAS
|-Signature Algorithm : MD5 With RSA Encryption
|-Valid From          : Aug 22 06:50:42 2007 GMT
|-Valid To            : Aug 21 06:50:42 2012 GMT
```

192.168.0.254 (tcp/443)

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiGate/CN=FGT40C3914025969/
E=support@fortinet.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 10 11:17:05 2014 GMT
|-Valid To            : Jan 19 03:14:07 2038 GMT
```

15901 (1) - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

192.168.0.251 (tcp/443)

```
The SSL certificate has already expired :

  Subject          : C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=TS Series NAS
  Issuer           : C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=TS Series NAS
  Not valid before : Aug 22 06:50:42 2007 GMT
  Not valid after  : Aug 21 06:50:42 2012 GMT
```

18405 (1) - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

http://www.oxid.it/downloads/rdp-gbu.pdf

http://www.nessus.org/u?e2628096

http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.6 (CVSS2#E:F/RL:W/RC:ND)

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Plugin Information:

Published: 2005/06/01, Modified: 2016/11/23

Plugin Output

192.168.0.84 (tcp/3389)

42873 (1) - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

192.168.0.254 (tcp/443)

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57690 (1) - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/01/25, Modified: 2018/01/29

Plugin Output

192.168.0.84 (tcp/3389)

```
The terminal services encryption level is set to :

2. Medium
```

58453 (1) - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

http://technet.microsoft.com/en-us/library/cc732713.aspx

http://www.nessus.org/u?e2628096

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2012/03/23, Modified: 2018/01/29

Plugin Output

192.168.0.84 (tcp/3389)

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

90317 (1) - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

192.168.0.254 (tcp/22)

```
The following weak server-to-client encryption algorithms are supported :

  arcfour

The following weak client-to-server encryption algorithms are supported :

  arcfour
```

70658 (2) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Published: 2013/10/28, Modified: 2016/05/12

Plugin Output

192.168.0.90 (tcp/22)

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
```

192.168.0.254 (tcp/22)

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

30218 (1) - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2008/02/11, Modified: 2018/01/29

Plugin Output

192.168.0.84 (tcp/3389)

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

33851 (1) - Network daemons not managed by the package system

Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

Risk Factor

Low

CVSS Base Score

2.1 (CVSS2#AV:N/AC:H/Au:S/C:N/I:P/A:N)

Plugin Information:

Published: 2008/08/08, Modified: 2017/08/28

Plugin Output

192.168.0.90 (tcp/0)

```
The following running daemons are not managed by RPM :

/usr/sbin/dhclient;5ac35977
/usr/sbin/dhclient;5ac35977
/usr/sbin/dhclient;5ac35977
/usr/sbin/dnsmasq;5ac35977
```

69551 (1) - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

192.168.0.254 (tcp/443)

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiGate/CN=FGT40C3914025969/
E=support@fortinet.com
|-RSA Key Length : 1024 bits
```

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

192.168.0.254 (tcp/22)

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
```