



資訊處
Office of Information Technology

設備弱掃後修補建議

中華民國112年10月

編號：

修補主要原則

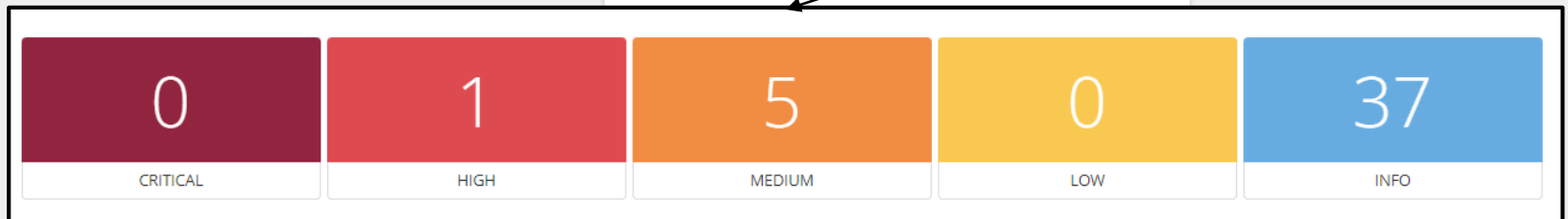
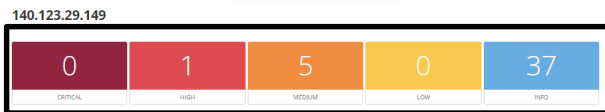
- 任何設備，如無須對外服務，建議本機端阻擋外部連線，或限制可連線來源
- 個人電腦/筆電/主機，請了解安裝哪些軟體、開啟哪些服務，並確認作業系統與軟體均已更新至最新
- 印表機/無線分享器/監視器等物聯網設備，請確保韌體更新至最新，並完成網路或安全性相關設定



資訊處
Office of Information Technology

如何閱讀報告

風險數統計



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.openwall.com/blog/2016/06/24/weak3d/>

統計目標IP弱點數與取得的資訊數
存在Critical(嚴重)、High(高)、Medium(中)弱點需盡速修補
存在Low(低)弱點僅為建議修補
Info(資訊)為弱掃工具取得該IP設備之服務資訊
目前的共識為中以上弱點都必須修補

```
Plugin Output
top/3389/mrmdp

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
Name Code KEX Auth Encryption MAC
-----
005-CBC1-SHA_0000_0000_RSA_RSA_3DES-CBC(168)_SHA1

The fields above are :
{[enable_ciphername]
{cipher_id_code]
Kex{key_exchange]
Auth{authentication]
Encrypt{symmetric_encryption_method]
MAC{message_authentication_code]
{export_flag]
```

弱點名稱與說明

140.123.29.149

0	1	5	0	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Aug 30 11:33:15 2023
End time: Wed Aug 30 11:44:24 2023

Host Information

Nebios Name: DESKTOP-AHQGM0BT
IP: 140.123.29.149
OS: Windows

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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.openstl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info/>

Solution

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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.

(Export: 418g)

57608 - SMB Signing not required

弱點的概述與特徵說明

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

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.

弱點參考連結與建議修補方式

140.123.29.149

0	1	5	0	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Aug 30 11:33:15 2023
End time: Wed Aug 30 11:44:24 2023

Host Information

Netbios Name: DESKTOP-AQGMOBT
IP: 140.123.29.149
OS: Windows

Vulnerabilities

42873 - 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/>
<https://sweet32.info/>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

57608 - SMB Signing not required

See Also : 提供弱點外部說明參考連結，會有較多針對弱點的特徵說明
Solution : 提供弱點修補建議

See Also

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

Solution

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

發現弱點的通訊埠



弱掃工具進行探測時發現設備開啟的通訊埠與其可能運行的服務較常見的通訊埠：

Tcp:21,22,80,135,139,443,445,3389,7070,8080,8443等
Udp:161等

https://www.openstf.org/blog/2015/08/24/weak32/
https://www.cve.org

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

Risk Factor
Medium

CVSS v3.0 Base Score
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score
6.1

CVSS v2.0 Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE [CVE-2016-2183](#)

Plugin Information
Published: 2009/11/23, Modified: 2017/02/03

Plugin Output
tcp/3389/msrdp

Medium Strength Ciphers (> 64-bit and < 128-bit key, or 3DES)
Name Code KEX Auth Encryption MAC

00S-CBC3-SHA_00W_00W RSA RSA_00S-CBC(128)_SHA1

The fields above are :
{(enable|ciphername)
{cipher|id|code}
Kex={key|exchange}
Auth={authentication}
Encrypt={symmetric|encryption|method}
MAC={message|authentication|code}
{export|flag}

57608 - SMB Signing not required

Plugin Output

tcp/3389/msrdp

還是看不懂？

➤ 請開啟瀏覽器並搜尋弱點名稱，大部分常見的狀況都能找到修補教學

The image shows two side-by-side browser windows. The left window displays a vulnerability page for '57608 - SMB Signing not required'. The right window shows a Google search result for the same term, with a red box highlighting a search result from 'pim0110.idv.tw' titled '修補弱點SMB Signing not required - 飛朵啦學習手札'. A red arrow points from the vulnerability name in the left window to the search result in the right window.

Vulnerabilities

57608 - SMB Signing not required

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

<http://www.nessus.org/u/df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u/774b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u/7a3cac4ea>

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 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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:O/RC:C)

Plugin Information

SMB Signing not required

約有 1,890,000 項結果 (搜尋時間: 0.19 秒)

修補弱點SMB Signing not required - 飛朵啦學習手札

2022年4月11日 — 開啟啟動登錄編輯器；點選左下角開始，於搜尋程式及檔案空白框，輸入「Regedit32.exe」指令。

How to resolve SMB Signing not required Vulnerability

The Purpose of this article is to share a quick way to resolve a vulnerability named SMB Signing not required .In most of the cases, when information ...

共享資料夾被nessus掃出SMB Signing not required中風險

如果像我一樣(如圖)找不到，那麼就要選擇 群組人員... 設定上傳權限的兩種方式(二選一)：設定資料夾共享權限

SMB Signing not required問題

2018年6月25日 — <<第一步驟>> 設定：停用TLS 1.0、TLS1.1服務。 開啟啟動登錄編輯器；點選左下角開始，於搜尋程式及檔案空白框，輸入「Regedit32.exe」指令。

SMB Signing not required vulnerability - Microsoft Q&A

已經搜尋過方法還是無法解決？

➤ 個人電腦/筆電/主機：

- ✓ 建議移除不常使用的軟體或關閉不常使用的服務
- ✓ 若無法解決問題，建議重灌設備，一台剛重灌未安裝軟體、未開啟對外服務且也更新到最新的電腦主機，基本上不會有弱點。

➤ 印表機/無線分享器/監視器等物聯網設備

- ✓ 進行設備韌體更新
- ✓ 安全性相關設定調校
- ✓ 設備網頁管理介面連線存取控制
- ✓ 若上述方式都無法進行，請改用私人網段(192.168)、改為單機作業或下架不使用



資訊處
Office of Information Technology

常見弱點項目

51192 – SSL Certificate Cannot Be Trusted

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 目前Let's Encrypt不被Nessus認為是信任憑證，若為網站或系統使用，本項可視為誤判
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

57582 – SSL Self-Signed Certificate

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

15901 – SSL Certificate Expiry

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略

104743 – TLS Version 1.0 Protocol Detection

- 若設備為**對外服務**之網站或系統，建議關閉TLS 1.0協定並啟用TLS 1.2以上協定
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

157288 – TLS Version 1.1 Protocol Deprecated

- 若設備為**對外服務**之網站或系統，建議關閉TLS 1.1協定並啟用TLS 1.2以上協定
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

- 若設備為**對外服務**之網站或系統，建議openssl避免使用中強度加密方法
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

41028 – SNMP Agent Default Community Name (public)

- 如用不到snmp功能，建議**停用**，或更改snmp社群名稱由public改成其他名稱
- 不同廠牌與設備設定不同，建議依產品手冊尋找設定位置，大多會在網路或安全性設定內

SNMP

警告：變更這些設定可能會中斷網路功能。

- 啟用 SNMP 讀寫權限。
- 啟用 SNMP 唯讀存取 (使用「public」做為 GET 社群名稱)。
- 停用 SNMP

SET 社群名稱:	<input type="text" value="anyothernames"/>	請取代「public」
確認 SET 社群名稱:	<input type="text"/>	
GET 社群名稱:	<input type="text"/>	
確認 GET 社群名稱:	<input type="text"/>	

停用 SNMP 預設 GET 及 SET 社群名稱「public」。

- 本項須由設備商釋出更新補丁，若設備商已不支援更新，建議改用私人網段(192.168.*.*)、改為單機作業或下架設備。

補充說明1 - windows遠端桌面連線

- 先檢查弱點項目的plugin output是否為tcp 3389

The image shows a screenshot of a vulnerability report for CVE-2016-2183. The report is divided into several sections: Solution, Risk Factor, Medium, CVSS v3.0 Base Score, VPR Score, CVSS v2.0 Base Score, References, Plugin Information, and Plugin Output. The Plugin Output section is highlighted with a box, and an arrow points from this box to a larger box on the right that contains the text 'Plugin Output' and 'tcp/3389/msrdp'.

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

Risk Factor
140.123.162.140 1187

Medium

CVSS v3.0 Base Score
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score
6.1

CVSS v2.0 Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References
CVE CVE-2016-2183

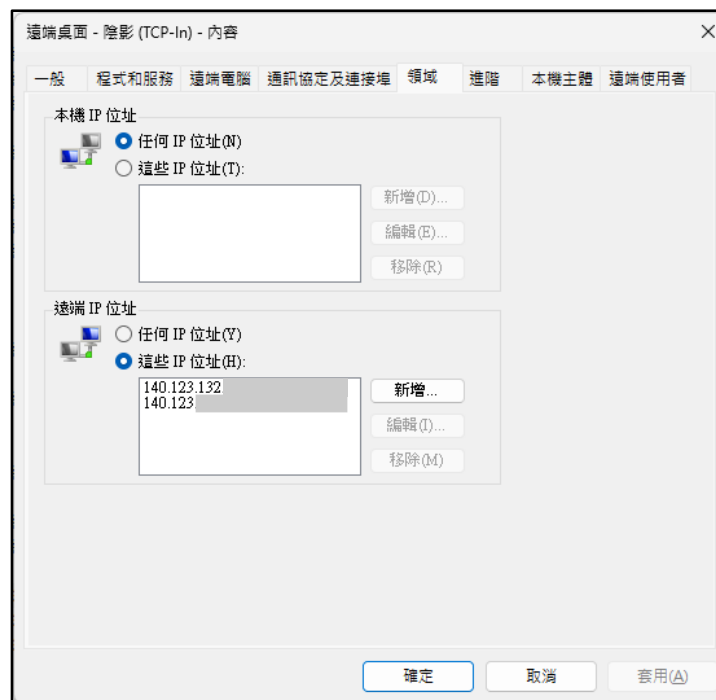
Plugin Information
Published: 2009/11/23 Modified: 2021/02/03

Plugin Output
tcp/3389/msrdp

Plugin Output
tcp/3389/msrdp

補充說明1 - windows遠端桌面連線

- 參考資訊處手冊p17~p27
- https://it.ccu.edu.tw/var/file/9/1009/img/Remote_Working_0607.pdf
- 建議依照手冊流程設定遠端來源IP-140.123.132.0/24或特定IP
- 學生vpn請設定140.123.3.0/24或特定IP





資訊處
Office of Information Technology

感謝閱讀

中正大學 資訊處