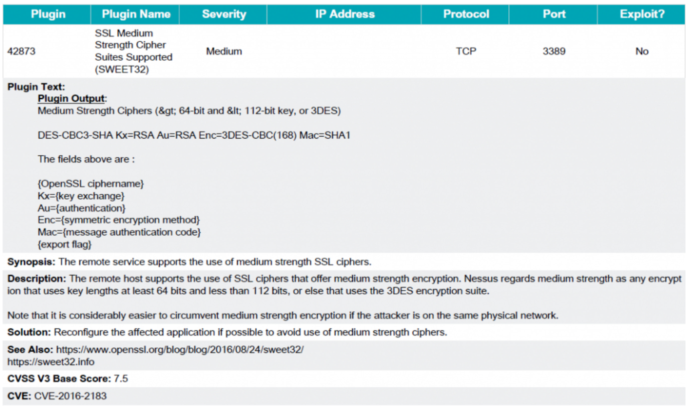
□□SSL Medium Strength Cipher Suites Supported (SWEET32)

□□□ Administrator
□□, 11 □□ 2022 11:20 - □□□□ □□, 22 □□ 2022 10:42

□□□□□
SSL Medium Strength Cipher Suites Supported (SWEET32)

□□□□□ 42873

□□□□□ □□



Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium		TCP	3389	No

Plugin Text:
Plugin Output:

```
Medium Strength Ciphers (&gt; 64-bit and &lt; 112-bit key, or 3DES)

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}
```

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.

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

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

CVSS V3 Base Score: 7.5

CVE: CVE-2016-2183

□□□□
□□□□□□□□□□□□□□□□SSL□□。
Nessus□□□□□□□□□□□□□□□□□□□□□64□□□□112□□□□□□□□□□□□□3DES□□□□□□□□□□。 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□。

□□□□

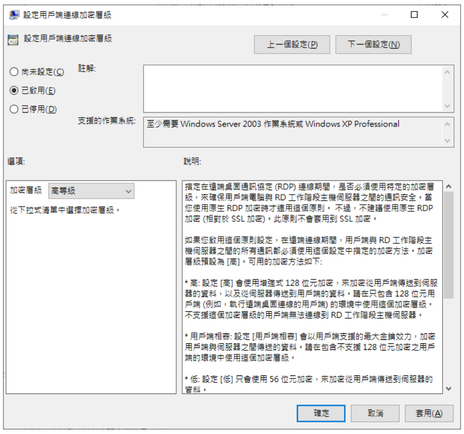
1. □□□□□□□□□□□Remote Desktop Protocol□RDP□□□□□□□□□。 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□「gpedit.msc」□□。

□□SSL Medium Strength Cipher Suites Supported (SWEET32)

□□□ Administrator
□□, 11 □□ 2022 11:20 - □□□□ □□, 22 □□ 2022 10:42

□□□□□□□□□□□□->□□□□->□□□□□□->Windows□□->□□□□□□->□□□□□□□□□□->□□□->□□□□□□□□□□□。

2. □□□□□□□□□□□。



○ 尚未設定(C)
● 已啟用(E)
○ 已停用(D)

支援的作業系統: 至少需要 Windows Server 2003 作業系統或 Windows XP Professional

加密層級: 高等級

從下拉式清單中選擇加密層級。

指定在遠端桌面通訊協定 (RDP) 連線期間，是否必須使用特定的加密層級，來確保用戶端電腦與 RD 工作階段主機伺服器之間的通訊安全。當您使用原生 RDP 加密時才適用這個原則。 不過，不建議使用原生 RDP 加密 (相對於 SSL 加密)。此原則不會套用到 SSL 加密。

如果您啟用這個原則設定，在遠端連線期間，用戶端與 RD 工作階段主機伺服器之間的所有通訊都必須使用這個設定中指定的加密方法。加密層級預設為 [高]。可用的加密方法如下:

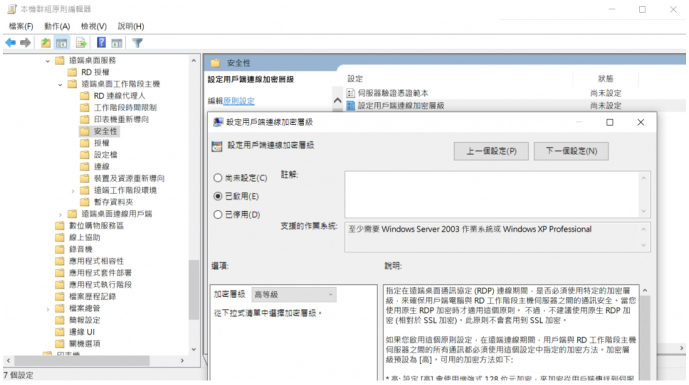
* 高: 設定 [高] 會使用增強式 128 位元加密，來加密從用戶端傳送到伺服器的資料，以及從伺服器傳送到用戶端的資料。請在只包含 128 位元用戶端 (例如，執行遠端桌面連線的用戶端) 的環境中使用這個加密層級。不支援這個加密層級的用戶端無法連線到 RD 工作階段主機伺服器。

* 用戶端相容: 設定 [用戶端相容] 會以用戶端支援的最大金鑰效力，加密用戶端與伺服器之間傳送的資料。請在包含不支援 128 位元加密之用戶端的環境中使用這個加密層級。

* 低: 設定 [低] 只會使用 56 位元加密，來加密從用戶端傳送到伺服器的資料。

3.

□□□□□□□3-DES□□□。 (For Windows)。



設定用戶端連線加密層級

設定	狀態
伺服器驗證憑證範本	尚未設定
設定用戶端連線加密層級	尚未設定

○ 尚未設定(C)
● 已啟用(E)
○ 已停用(D)

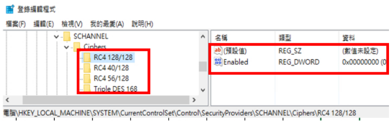
支援的作業系統: 至少需要 Windows Server 2003 作業系統或 Windows XP Professional

加密層級: 高等級

從下拉式清單中選擇加密層級。

指定在遠端桌面通訊協定 (RDP) 連線期間，是否必須使用特定的加密層級，來確保用戶端電腦與 RD 工作階段主機伺服器之間的通訊安全。當您使用原生 RDP 加密時才適用這個原則。 不過，不建議使用原生 RDP 加密 (相對於 SSL 加密)。此原則不會套用到 SSL 加密。

如果您啟用這個原則設定，在遠端連線期間，用戶端與 RD 工作階段主機伺服器之間的所有通訊都必須使用這個設定中指定的加密方法。加密層級預設為 [高]。可用的加密方法如下:



名稱	類型	資料
(預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0

電腦\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128

□□□
□□□□□□□□□□□□□□□□□□□□□□Windows□□□□□□。

Linux□□、 SQL、 IIS□□□□□□□□□□□□□□□□□□□□□□□□。

□□SSL□□□□GOOGLE□□□□□□□□。

□□□ https://ithelp.ithome.com.tw/articles/10249216

□□□□□□□□□□□□□□□□□□windows□□□□□□□□□□□IISCrypto.exe□□□□□□□□□□□□□。
□□□□ https://www.nartac.com/Products/IISCrypto

□□□□□ https://social.technet.microsoft.com/wiki/contents/articles/52234.exchange-2016-cipher-lockdown-with-iiscrypto-2-0.aspx?Redirected=true