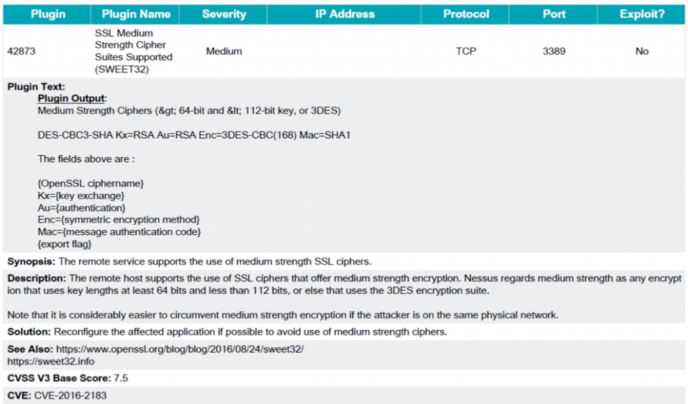


修補 SSL Medium Strength Cipher Suites Supported (SWEET32)

作者是 Administrator
週一 , 11 四月 2022 11:20 - 最近更新 週五 , 22 四月 2022 10:42

弱點名稱:

SSL Medium Strength Cipher Suites Supported (SWEET32)

插件編號: 42873

風險程度: 中等

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 (> 64-bit and < 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

風險原因:

伺服器支援使用提供中等強度加密的 SSL密碼 。

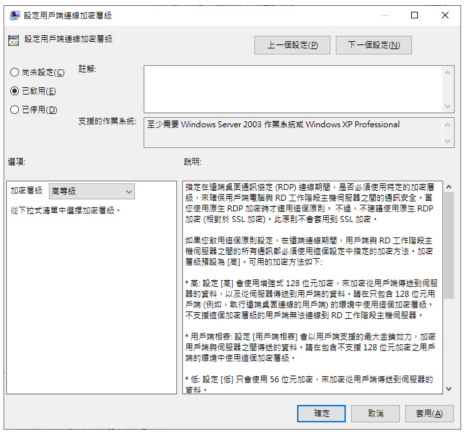
Nessus檢測原則將中等強度視為使用密鑰長度至少 64位且小於 112位的任何加密，或者使用 3DES加密套件的任何加密 。 請注意，如果攻擊者在同一物理網絡上，則規避中等強度的加密非常容易 。

修補方式:

1. 設定：遠端桌面協定（Remote Desktop Protocol，RDP）安全性為高層級 。 開啟本機群組原則編輯器：點選左下角開始，於搜尋程式及檔案空白框，輸入 「gpedit.msc」 指令 。

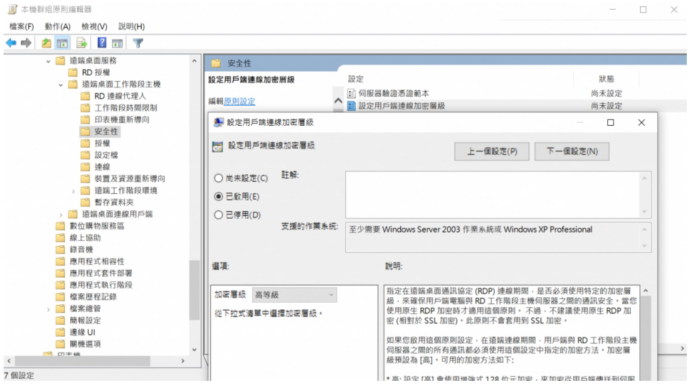
路徑：本機群組原則編輯器 ->電腦設定 ->系統管理範本 ->Windows元件 ->遠端桌面服務 ->遠端桌面工作階段主機 ->安全性 ->設定用戶端連線加密層級 。

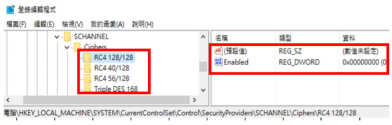
2. 將其設定為高層級如下圖 。



3.

透過登錄檔移除 3-DES演算法 。 (For Windows)。





備註:

這個弱點觸發的原因很多，上面提供的解法僅限於 Windows系統本身漏洞 。

Linux系統 、 SQL、 IIS等其他應用程式服務的解法各有不同我就不列舉出來了 。

今天光修補這隻弱點就碰到很多瓶頸，相同的修補方式有些機器沒有解除，經檢查之後發現原來是其他應用程式服務也有使用到這些 SSL，幸好有 GOOGLE大神才知道怎麼解 。

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

若是嫌登錄檔操作麻煩，而電腦又是使用 windows系統，那麼建議可以使用 IISCrypto.exe，這個可操作圖形化介面工具 。
下載點: https://www.nartac.com/Products/IISCrypto

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