

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。

Nessus641123DES。。

- Remote Desktop ProtocolRDP。。「gpedit.msc」。

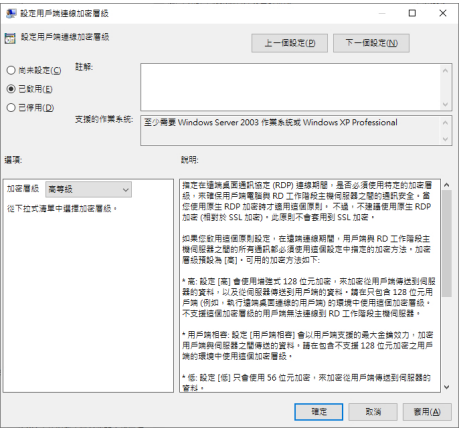
SSL Medium Strength Cipher Suites Supported (SWEET32)

Administrator

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

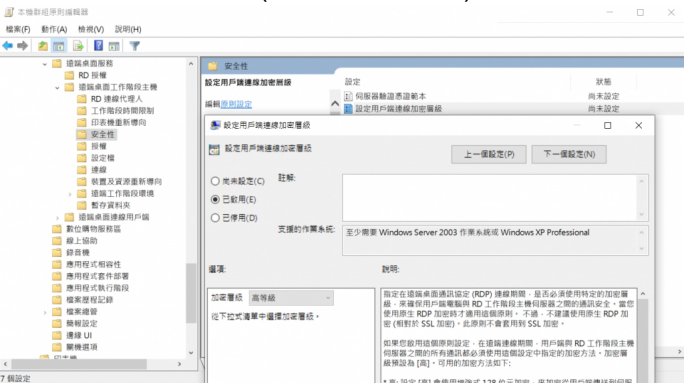
Windows

2.



3.

3-DES (For Windows).



名稱	類型	資料
RC4 128/128	RC4_128	RC4 128/128
RC4 40/128	RC4_40	RC4 40/128
RC4 160/128	RC4_160	RC4 160/128
Triple DES 168	TripleDES_168	Triple DES 168

Windows

SSL Medium Strength Cipher Suites Supported (SWEET32)

Administrator

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

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>