HIGH SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Output

```
- SSLv3 is enabled and the server supports at least one cipher.
        Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                    Kx=RSA        Au=RSA      Enc=RC4(128)              Mac=MD5
    RC4-SHA                    Kx=RSA        Au=RSA      Enc=RC4(128)
Mac=SHA1

The fields above are :

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

Port	Hosts
4433 / tcp / www	[redacted]
443 / tcp / www	[redacted]

Plugin Details

Severity:	High
ID:	20007
Version:	1.32
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	March 27, 2019

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS Base Score: 7.1
CVSS Vector:
CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N

Vulnerability Information

In the news: true