Report generated by Nessus™

scan meta completo

Sun, 27 Aug 2023 12:50:46 EDT

VULNERABILITY

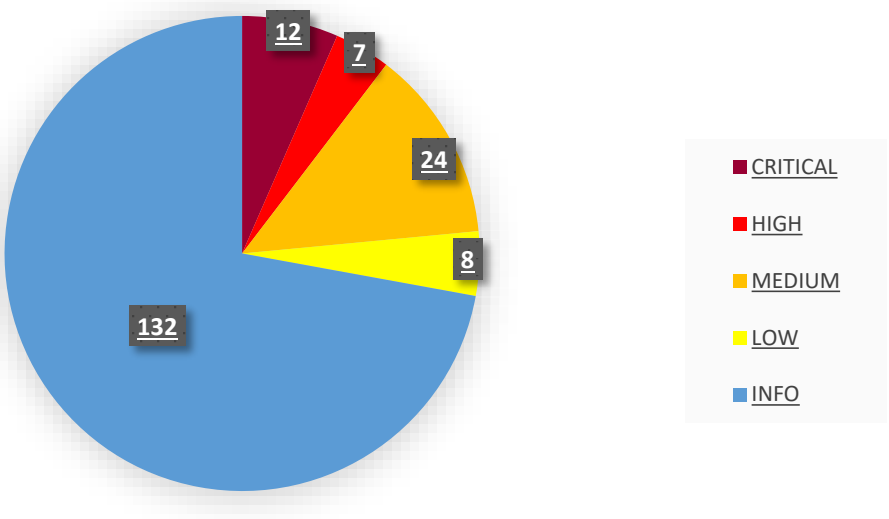

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.31.100

CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sun Aug 27 12:32:05 2023

End time: Sun Aug 27 12:50:46 2023

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.31.100

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

56134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis : There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor High

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score 9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score 9.2

CVSS v2.0 Base Score 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score 6.5 (CVSS2#E:H/RL:OF/RC:C)

171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score 10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

51988 - Bind Shell Backdoor Detection

Synopsis The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor Critical

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis : The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor Critical

VPR Score 7.4

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

Exploitable With Core Impact (true)

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis : The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor Critical

VPR Score 7.4

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

Exploitable With Core Impact (true)

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor Critical

VPR Score 7.4

CVSS v2.0 Base Score10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

Exploitable With Core Impact (true)

11356 - NFS Exported Share Information Disclosure

Synopsis : It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor Critical

VPR Score 5.9

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

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 1.2 (with approved cipher suites) or higher instead.

Risk Factor Critical

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis : The remote service encrypts traffic using a protocol with known weaknesses.

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 1.2 (with approved cipher suites) or higher instead.

Risk Factor Critical

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.3

Solution Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor Critical

CVSS v3.0 Base Score 10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

46882 - UnrealIRCd Backdoor Detection

Synopsis The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor Critical

VPR Score 7.4

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score 8.3 (CVSS2#E:F/RL:OF/RC:C)

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution Secure the VNC service with a strong password.

Risk Factor Critical

CVSS v2.0 Base Score 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

136769 - ISC BIND Service Downgrade / Reflected DoS

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.
An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor Medium

CVSS v3.0 Base Score 8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score 7.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 5.2

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

CVSS v2.0 Temporal Score 3.7 (CVSS2#E:U/RL:OF/RC:C)

42256 - NFS Shares World Readable

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution

Place the appropriate restrictions on all NFS shares.

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)

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

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.

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)

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.

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)

90509 - Samba Badlock Vulnerability

Synopsis : An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor Medium

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

CVSS v3.0 Temporal Score 6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 6.7

CVSS v2.0 Base Score 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score 5.0 (CVSS2#E:U/RL:OF/RC:C)

10205 - rlogin Service Detection

Synopsis : The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor High

VPR Score 6.7

CVSS v2.0 Base Score 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

10245 - rsh Service Detection

Synopsis

The rsh service is running on the remote host.

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor High

VPR Score 6.7

CVSS v2.0 Base Score 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Exploitable With Metasploit (true)

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Risk Factor Medium

CVSS v3.0 Base Score 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

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

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor Medium

CVSS v3.0 Base Score 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score 4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 4.0

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

CVSS v2.0 Temporal Score 3.7 (CVSS2#E:U/RL:OF/RC:C)

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Synopsis

The remote name server is affected by a denial of service vulnerability.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution : Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score 5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 3.6

CVSS v2.0 Base Score 4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score 3.0 (CVSS2#E:U/RL:OF/RC:C)

136808 - ISC BIND Denial of Service

Synopsis

The remote name server is affected by an assertion failure vulnerability.

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to the patched release most closely related to your current version of BIND.

Risk Factor Medium

CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score 5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score 5.1

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score 3.4 (CVSS2#E:POC/RL:OF/RC:C)

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.

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/C:N/I:P/A:N)

CVSS v2.0 Temporal Score 3.7 (CVSS2#E:U/RL:OF/RC:C)

52611 - SMTP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.
Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

Solution Contact the vendor to see if an update is available.

Risk Factor Medium

VPR Score 6.3

CVSS v2.0 Base Score 4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score 3.1 (CVSS2#E:POC/RL:OF/RC:C)

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor Medium

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

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

Risk Factor Low

CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score 5.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 3.6

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 1.9 (CVSS2#E:U/RL:OF/RC:C)

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution Purchase or generate a proper SSL certificate for this service.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution Purchase or generate a proper SSL certificate for this service.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

15901 - SSL Certificate Expiry

Synopsis : The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution Purchase or generate a new SSL certificate to replace the existing one.

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

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

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

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution : Purchase or generate a proper SSL certificate for this service.

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

45411 - SSL Certificate with Wrong Hostname

Synopsis : The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution Purchase or generate a proper SSL certificate for this service.

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

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Risk Factor Medium

CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score 5.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 4.4

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 3.2 (CVSS2#E:U/RL:OF/RC:C)

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis : The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor Medium

CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score 5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score 3.6

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 3.7 (CVSS2#E:U/RL:ND/RC:C)

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis : The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor Medium

CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score 5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score 3.6

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 3.7 (CVSS2#E:U/RL:ND/RC:C)

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution Purchase or generate a proper SSL certificate for this service.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution Purchase or generate a proper SSL certificate for this service.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor Medium

CVSS v3.0 Base Score 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

Solution : Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor Medium

VPR Score 4.5

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score 3.2 (CVSS2#E:U/RL:OF/RC:C)

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
SolutionEnable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score 6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
Solution : Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score 6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.
SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution : Disable the Telnet service and use SSH instead.

Risk Factor Medium

CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor Low

VPR Score 2.5

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 1.9 (CVSS2#E:U/RL:OF/RC:C)

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.
This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
gss-gex-sha1-*
gss-group1-sha1-*
gss-group14-sha1-*
rsa1024-sha1
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution : Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor Low

CVSS v3.0 Base Score 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor Low

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor Low

CVSS v3.0 Base Score 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score 3.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 4.5

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score 1.9 (CVSS2#E:U/RL:OF/RC:C)

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor Low

CVSS v3.0 Base Score 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score 3.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score 4.5

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score 2.2 (CVSS2#E:U/RL:ND/RC:C)

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.
As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.
The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.
This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation.
Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Solution

Disable SSLv3.
Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor Medium

CVSS v3.0 Base Score 3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

CVSS v3.0 Temporal Score 3.1 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score 5.3

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 3.4 (CVSS2#E:POC/RL:OF/RC:C)

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.
As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.
The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.
This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation.
Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Solution

Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor Medium

CVSS v3.0 Base Score 3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

CVSS v3.0 Temporal Score 3.1 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score 5.3

CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score 3.4 (CVSS2#E:POC/RL:OF/RC:C)

10407 - X Server Detection

Synopsis : An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.
Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution : Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor Low

CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N).

Vulnerabilità “ Info “

Le vulnerabilità "Info" rilevate da Nessus non corrispondono a una minaccia immediata per la sicurezza, ma forniscono informazioni rilevanti alla configurazione della macchina o del sistema come ad esempio : banner di servizio / informazioni sui certificati / note generali , o info in generale.