CRITIC

9.8 9.2 134862 Apache Tomcat A JP Connector Request Injection (Ghostcat)

9.8 - 51988 Bind Shell Backdoor Detection

9.8 - 20007 SSL Version 2 and 3 Protocol Detection

9.1 6.0 33447 Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

10.0 - 171340 Apache Tomcat SEoL (<= 5.5.x)

10.0 - 33850 Unix Operating System Unsupported Version Detection

10.0* 7.4 32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

10.0* 7.4 32321 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

10.0* 5.9 11356 NFS Exported Share Information Disclosure

10.0* - 61708 VNC Server 'password' Password

8.6 5.2 136769 ISC BIND Service Downgrade / Reflected DoS

7.5 - 42256 NFS Shares World Readable

7.5 6.1 42873 SSL Medium Strength Cipher Suites Supported (SWEET32)

7.5 6.7 90509 Samba Badlock Vulnerability

7.5* 6.7 10205 rlogin Service Detection

7.5* 6.7 10245 rsh Service Detection

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.

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

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cip

Contact your DNS server vendor for a patch.

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

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

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.

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.

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

Secure the VNC service with a strong password.

Middle

6.5 3.6 139915 ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

6.5 - 51192 SSL Certificate Cannot Be Trusted

192.168.1.4 4

6.5 - 57582 SSL Self-Signed Certificate

6.5 - 104743 TLS Version 1.0 Protocol Detection

6.5 - 42263 Unencrypted Telnet Server

5.9 5.1 136808 ISC BIND Denial of Service

5.9 3.6 31705 SSL Anonymous Cipher Suites Supported

5.9 4.4 89058 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

5.9 3.6 65821 SSL RC4 Cipher Suites Supported (Bar Mitzvah)

5.3 - 12085 Apache Tomcat Default Files

5.3 - 12217 DNS Server Cache Snooping Remote Information Disclosure

5.3 4.0 11213 HTTP TRACE / TRACK Methods Allowed

5.3 - 57608 SMB Signing not required

5.3 - 15901 SSL Certificate Expiry

5.3 - 45411 SSL Certificate with Wrong Hostname

5.3 - 26928 SSL Weak Cipher Suites Supported

4.0* 6.3 52611 SMTP Service STARTTLS Plaintext Command Injection

4.3* - 90317 SSH Weak Algorithms Supported

4.3* 4.5 81606 SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Solutions

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Purchase or generate a proper SSL certificate for this service.

Purchase or generate a proper SSL certificate for this seEnable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.rvice.

Disable the Telnet service and use SSH instead.

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

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

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.

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.

Contact the vendor of the DNS software for a fix.

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

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

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

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

Contact the vendor to see if an update is available.

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

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Low

153953 SSH Weak Key Exchange Algorithms Enabled
3.7 4.5 83875 SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
3.7 4.5 83738 SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
3.4 5.3 78479 SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
2.6* 2.5 70658 SSH Server CBC Mode Ciphers Enabled
2.6* - 71049 SSH Weak MAC Algorithms Enabled
2.6* - 10407 X Server Detection
192.168.1.4

solutions

Contact the vendor or consult product documentation to disable the weak algo

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

See Alsorithms.

Reconfigure the service to use a unique Diffieeconfigure the service to remove support for EXPORT_DHE cipher suites.-Hellman moduli of 2048 bits or grDisable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.eater.Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

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

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