# critiche

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

## SOLUZIONi

134862 Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

51988 Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

20007 "porta vulnerabile ssl" Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0.

Utilizzare invece TLS 1.2 (con suite di crittografia approvate) o superiore.

33447 Contattare il fornitore del server DNS per una patch.

171340 Eseguire l'aggiornamento a una versione di Apache Tomcat attualmente supportata.

33850 Eseguire l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.

32314 Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale chiavConsiderare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigeneratoe SSH, SSL e OpenVPN dovrebbe essere rigenerato. (altra porta vulnerabile)

32321 (altra porta vulnerabile)Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato

11356 Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le proprie condivisioni remote.

61708 Proteggi il servizio VNC con una password complessa.

136769 Eseguire l'aggiornamento alla versione ISC BIND a cui si fa riferimento nell'advisory del fornitore.

42256 Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie di media intensità.

42873 Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie di media intensità.(PORTA)

90509 Aggiornamento a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

10205 Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare SSH.

10245 Commentare la riga 'rsh' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare SSH.

# MEDIE

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
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)

# soluzionI

139915 Aggiornamento a BIND 9.11.22, 9.16.6, 9.17.4 o versione successiva.
51192 Acquista o genera un certificato SSL appropriato per questo servizio.
57582 Acquista o genera un certificato SSL appropriato per questo servizio.
104743 Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.
42263 Disattivare il servizio Telnet e utilizzare SSH.
136808 Disattivare il servizio Telnet e utilizzare SSH.
31705 Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di codici deboli.
89058 Disabilitare SSLv2 ed esportare suite di crittografia crittografica. Assicurarsi che le chiavi private non vengano utilizzate ovunque con software server che supporta connessioni SSLv2.
65821Riconfigurare l'applicazione interessata, se possibile, per evitare l'utilizzo di crittografie RC4. Prendi in considerazione l'utilizzo di TLS 1.2 con suite AES-GCM soggette al supporto di browser e server Web.
12085 Eliminare la pagina indice predefinita e rimuovere l'esempio JSP e servlets. Seguire le istruzioni Tomcat o OWASP per sostituire o modificare la pagina di errore predefinita.

12217 Contattare il fornitore del software DNS per una correzione.
11213 Disattivare questi metodi HTTP. Fare riferimento all'output del plugin per ulteriori informazioni.
57608 Applicare la firma dei messaggi nella configurazione dell'host. In Windows, si trova nell'impostazione dei criteri "Server di rete Microsoft: comunicazioni con firma digitale (sempre)". Su Samba, l'impostazione è chiamata "firma del server". Vedi i link "vedi anche" per ulteriori dettagli.
15901 Acquista o genera un nuovo certificato SSL per sostituire quello esistente.
45411 Acquista o genera un certificato SSL appropriato per questo servizio.
26928 Riconfigurare l'applicazione interessata, se possibile per evitare l'utilizzo di codici deboli.
52611 Contattare il fornitore per verificare se è disponibile un aggiornamento.
90317 Contattare il fornitore o consultare la documentazione del prodotto per rimuovere i codici deboli.
81606 Riconfigurare il servizio per rimuovere il supporto per EXPORT_RSA suite di crittografia.

# bassi

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

# soluzione

153953 Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi deboli.

83875 Riconfigurare il servizio per utilizzare un modulo Diffie-Hellman univoco di 2048 bit o superiore.

83738 Riconfigurare il servizio per rimuovere il supporto per EXPORT_DHE suite di crittografia.

78479 Disabilitare SSLv3.I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS fino a quando SSLv3 non può essere disabilitato.

70658 Contattare il fornitore o consultare la documentazione del prodotto per disabilitare la crittografia in modalità CBC e abilitare la crittografia in modalità di crittografia CTR o GCM

71049 Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MD5 e MAC a 96 bit.

10407 Limitare l'accesso a questa porta. Se la funzione client/server X11 non viene utilizzata, disabilitare completamente il supporto TCP in X11 (-nolisten tcp).

le porte sono tutte quelle con: ssl e ssh