REPORT TECNICO

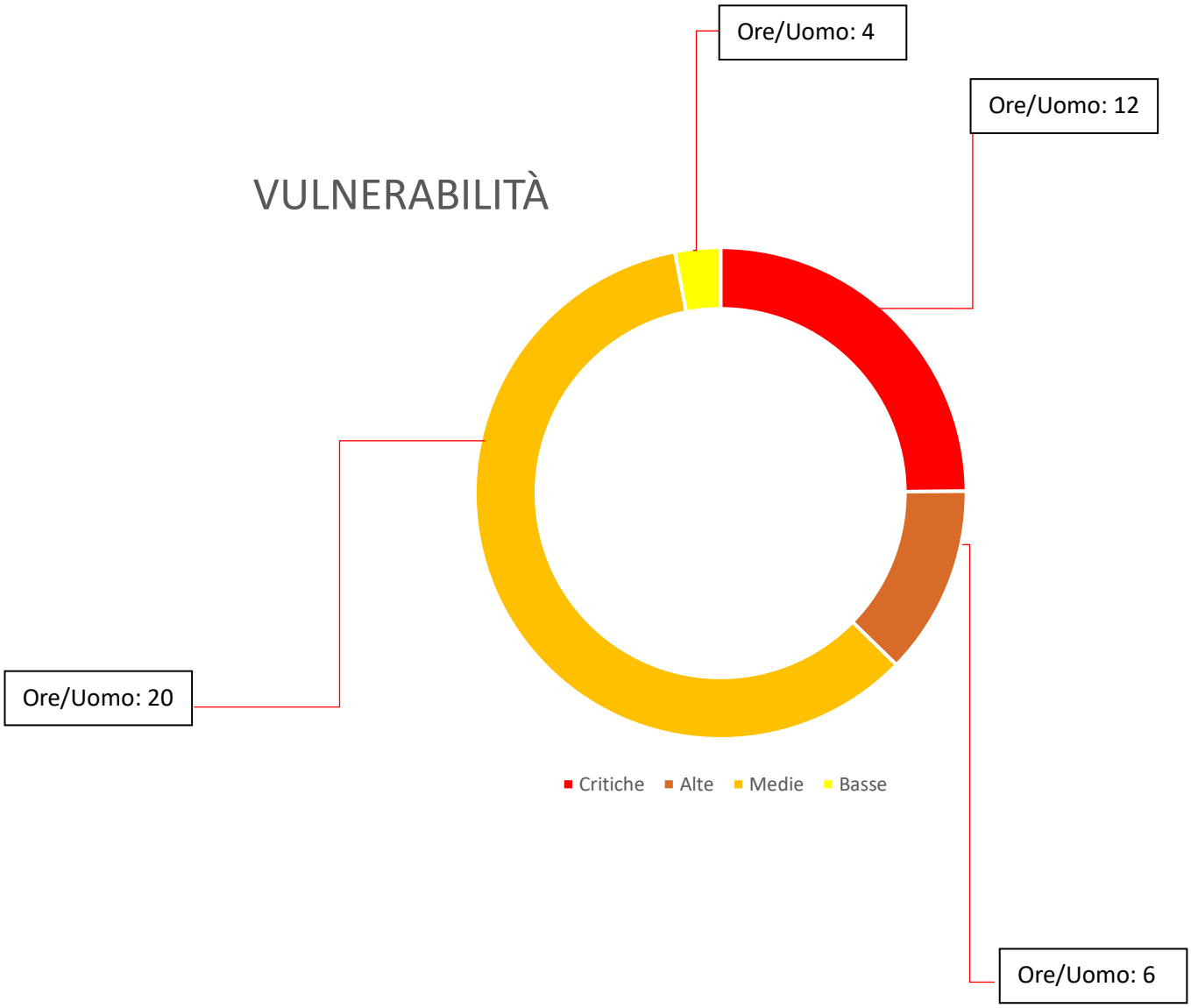
Target → [redacted]

IP: 192.168.50.101 **MAC**: 08:00:27:7F:1D:B7

Scansione sulle porte più comuni.

Ore/uomo totali stimate: 42 h

Vulnerabilità individuate:



VULNERABILITÀ CRITICHE:

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

L'Apache JServ Protocol (AJP) è un metodo per un server web per comunicare con un server di applicazione associata. Il server web è un "proxy inverso," significato, il suo scopo è di gestire il traffico in arrivo da Internet per conto del server di applicazione. Un attaccante, anche se non autenticato, può sfruttare questa debolezza per accedere ai file o addirittura utilizzare JSP (Java Server Pages) per ottenere il controllo remoto del server.

Porta: 8009

Soluzione: Update della configurazione AJP in modo tale da richiedere autorizzazione e/o upgrade del server Tomcat almeno alla versione 7.0.100

51988 - Bind Shell Backdoor Detection

L'host potrebbe risultare compromesso da una backdoor nel sistema. Una shell è in ascolto e un attaccante potrebbe servirsene per accedervi da remoto ed inviare comandi.

Porta: 1524

Soluzione: Verifica della compromissione dell'host. Reinsatallazione del sistema se necessario.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Le ssh key sono chiavi crittografiche che utilizzano un sistema crittografico a chiave pubblica, definiscono chi può accedere a ciascun sistema. Le chiavi di accesso del sistema risultano deboli. Inoltre sembrano contenere dei bug nel generatore randomico o nella OpenSSL (OpenSSL è una libreria software open source ampiamente utilizzata per generare e gestire certificati). Come risultato della debolezza, acune chiavi crittografate risultano essere più comuni di quanto effettivamente debbano essere. Il problema è attribuibile ad un pacchetto Debian che rimuove la casualità e l'entropia nella versione remota di OpenSSL.

Un attaccante può sfruttare un attacco brute force avendo discreta conoscenza del sistema oppure ottenere la parte privata della chiave, usandola per decifrare la sessione.

Porta: 22

Soluzione: andrebbero considerati tutto ciò che viene generato dal sistema come indovinabile. Andrebbero rigenerati tutti i protocolli SSH, SSL e OpenVPN.

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

Il certificato x509 è stato generato da un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri o nella libreria OpenSSL.

Porta: 25

Vedi 32321.

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

Il certificato x509 è stato generato da un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri o nella libreria OpenSSL.

Porta 5432.

Vedi 32321.

11356 - NFS Exported Share Information Disclosure

L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale. Il NFS permette ai calcolatori che compongono un sistema distribuito di condividere file, directory o un intero file system utilizzando il protocollo client-server. Un calcolatore (client) deve richiedere esplicitamente ad un altro calcolatore (server) del sistema distribuito di condividere una directory o un file, dichiarando un punto di montaggio. Una volta effettuato un montaggio un utente sul calcolatore client accede alla directory montata in modo assolutamente trasparente, ossia accede alla directory remota credendo di accedere ad una directory locale.

Un attaccante può utilizzare la vulnerabilità presente nel server remoto per leggere o scrivere i file nell'host.

Porta: 2049

Soluzione: configurare l'NFS sull'host remoto in modo tale che solo gli host autorizzati possano avere accesso alle sue condivisioni.

20007 - SSL Version 2 and 3 Protocol Detection

Il servizio SSL v.2 e 3 utilizzano un protocollo con debolezze conosciute come uno schema di "padding" (ovvero il processo di preparazione del messaggio alla criptazione) piuttosto debole ed una rinegoziazione e ripresa della sessione debole. Un attaccante può sfruttare la vulnerabilità per condurre un attacco con man-in-the-middle oppure decriptare le comunicazioni fra il servizio SSL2/3 e client.

È stato determinato dal NIST (National Institute of Standards and Technology) che il protocollo SSL3 non è più accettabile per le comunicazioni sicure. È consigliabile disabilitare del tutto i protocolli in questione.

Porta: 25

20007 - SSL Version 2 and 3 Protocol Detection

Porta: 5432

Vedi 20007

33850 - Unix Operating System Unsupported Version Detection

Il Sistema operativo sull'host non è più supportato. La mancanza di supporto si esplica anche nell'assenza di patch di sicurezza da parte del vendor sull'host in questione. È probabile che la versione in questione abbia forti debolezze sul piano della sicurezza.

Porta: 0

Soluzione: upgrade alla versione di Unix correntemente supportata.

61708 - VNC Server 'password' Password

Il server VNC (Virtual Network Computing) ha la copertura di una password debole (password). Lo scanner Nessus è riuscito ad accedervi. È possibile che anche un attaccante remoto sfrutti la debolezza della password per accedere.

Porta: 5900

Soluzione: cambia password gentilmente.

VULNERABILITÀ ALTE:

136769 - ISC BIND Service Downgrade / Reflected DoS

Un attacco downgrade è una tipologia di attacco che provoca il drop ad una versione precedente di una connessione, un protocollo o un algoritmo crittografico. È anche chiamato “Rollback Attack” o “Bidding-Down Attack”. L’attacco mira a sfruttare vulnerabilità che affliggono le versioni precedenti del materiale che si vuole aggredire. Reflected Denial of Service fa uso di un componente terzo potenzialmente legittimo per inviare il traffico dell’attacco a una vittima, nascondendo in ultima analisi l’identità degli aggressori. Il “componente terzo” può essere un pc, una stampante, una telecamera, un server o qualsiasi elemento attivo che possa essere sfruttato.

Porta: 53

Soluzione: upgrade del ISC BIND (BIND - Berkeley Internet Name Domain - è il server DNS più usato su Internet, specialmente sui sistemi Unix e derivati, sui quali è lo standard di fatto).

42256 - NFS Shares World Readable

L’ NFS è un protocollo di servizio file che consente agli utenti di accedere ai file su un server remoto, rendendolo un file system distribuito. Il server NFS di questo sistema può esportare senza restringere gli accessi possibili (ad esempio indirizzo IP, range di indirizzi IP, o basati su hostname).

Porta: 2049

Soluzione: aggiornare le restrizioni sull’accesso ai file dal NFS.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Il protocollo SSL utilizza una cifratura media (tra i 64 e i 112 bits) o una encryption suite (algoritmi utilizzati per rendere sicuri i collegamenti di rete basati su Transport Layer Security o sul suo predecessore, ora deprecato, Secure Socket Layer) di tipo 3DES.

Porta: 25

Soluzione: riconfigurare l’applicazione utilizzando una cifratura di forza superiore.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Porta: 5432

Vedi sopra

90509 - Samba Badlock Vulnerability

Il server SMB è affetto dalla vulnerabilità “Badlock”, che affligge il SAM (Security Account Manager) e il LSAD (Local Security Authority Domain Policy). Un attaccante in grado di intercettare il traffico fra un client e un host con servizio SAM può sfruttare questa vulnerabilità per fare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database di Active Directory (AD) o la disabilitazione servizi critici.

Porta: 445

Soluzione: Upgrade a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successive.

VULNERABILITÀ MEDIE:

11213 - HTTP TRACE / TRACK Methods Allowed

Le funzioni di debug sono abilitate sul server Web remoto. Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi http utilizzati per eseguire il debug delle connessioni del server Web.

Porta: 80

Soluzione: Disabilita questi metodi http.

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

Il server remote è affetto dalla vulnerabilità DoS – Denial of Service. Il server è, quindi, influenzato da una vulnerabilità di negazione del servizio (DoS) dovuta a un errore di asserzione durante il tentativo di verificare un file troncato risposta a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando un file risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando l'uscita dal server.

Porta: 53

Soluzione: Upgrade a BIND 9.11.22, 9.16.6, 9.17.4 o successive.

136808 - ISC BIND Denial of Service

Il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione. [da Microsoft.com: Un'asserzione software specifica una condizione che si prevede abbia valore True in un particolare punto del programma. Se un'asserzione sull'ora di compilazione non riesce, il compilatore genera un messaggio di diagnostica e un errore di compilazione. Se un'asserzione di runtime non riesce, il sistema operativo genera un messaggio di diagnostica e chiude l'applicazione. Esiste una vulnerabilità Denial of Service (DoS) nelle versioni ISC BIND 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 e precedenti. Un attaccante non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere.

Porta: 53

Soluzione: Aggiorna alla versione con patch più vicina alla tua attuale versione di BIND.

57608 - SMB Signing not required

La firma non è richiesta sul server SMB remoto. La firma non è richiesta sul server SMB remoto. Un attaccante può sfruttarlo per condurre attacchi “man-in-the-middle” contro il server SMB.

Porta: 445

Soluzione: Rafforza la sicurezza imponendo la firma dei messaggi nella configurazione dell'host. Su Windows, questo si trova nell'impostazione dei criteri 'Server di rete Microsoft: firmare digitalmente le comunicazioni (sempre)'. Su Samba, l'impostazione si chiama 'server firma'.

52611 - SMTP Service STARTTLS Plaintext Command Injection

Il servizio di posta remota consente l’inserimento di comandi in testo normale durante la negoziazione di un canale crittografato di comunicazione. Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire ad un attaccante di iniettare comandi durante la fase del protocollo in chiaro che sarà successivamente eseguito durante la fase del protocollo del testo cifrato. Un attacco riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o SASL (Simple Authentication and Security Layer) o le credenziali di autenticazione e del livello di sicurezza.

Porta: 25

Soluzione: Controllare se sono disponibili aggiornamenti tramite il fornitore.

90317 - SSH Weak Algorithms Supported

Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo. Nessus ha rilevato che il server SSH remoto è configurato per utilizzare la cifratura a flusso Arcfour o nessuna cifratura. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con chiavi deboli.

Porta: 22

Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifrature deboli

31705 - SSL Anonymous Cipher Suites Supported

Il servizio remoto supporta l'uso di cifrari SSL anonimi. L'host remoto supporta l'uso di cifrari SSL anonimi. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.

Nota: questo è molto più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica.

Porta: 25

Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature deboli.

51192 - SSL Certificate Cannot Be Trusted

Il certificato SSL per questo servizio non può essere ritenuto attendibile. Il certificato X.509 del server non può essere attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la “catena della fiducia” può essere spezzata, come indicato di seguito:

- Innanzitutto, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi quando la parte superiore della catena è un'autofirmata non riconosciuta certificato o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.

- In secondo luogo, la catena di certificati potrebbe contenere un certificato non valido al momento della scansione. Ciò può verificarsi quando la scansione avviene prima di una delle date "notBefore" del certificato o dopo una delle date "notAfter" del certificato.

- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrispondeva alle informazioni del certificato o che non poteva essere verificata. Le firme errate possono essere corrette facendo firmare nuovamente il certificato con la firma errata dall'emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato di un algoritmo di firma che Nessus non supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-themiddle contro l'host remoto.

Porta: 25

Soluzione: Acquista o genera un certificato SSL appropriato per questo servizio.

51192 - SSL Certificate Cannot Be Trusted

Vedi sopra

Porta: 5432

15901 - SSL Certificate Expiry

Il certificato SSL del server remoto è scaduto.

Porta: 25

Soluzione: Acquista o genera un nuovo certificato SSL per sostituire quello esistente.

15901 - SSL Certificate Expiry

Vedi sopra

Porta: 5432

45411 - SSL Certificate with Wrong Hostname

Il certificato SSL per questo servizio è per un host diverso. L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa.

Porta: 25

Soluzione: Acquista o genera un nuovo certificato SSL per sostituire quello esistente.

45411 - SSL Certificate with Wrong Hostname

Vedi sopra

Porta: 5432

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

L'host remoto potrebbe essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS acquisitor. L'host remoto supporta SSLv2 e pertanto può essere affetto da una vulnerabilità che consente un attacco crossprotocol Bleichenbacher padding oracle noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione di Secure Sockets Layer Version 2 (SSLv2) e consente la decrittografia del traffico TLS acquisito. Un utente malintenzionato man-in-the-middle può sfruttarlo per decrittografare la connessione TLS utilizzando traffico acquisito in precedenza e crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.

Porta: 25

Soluzione: Disabilita SSLv2 ed esporta le suite di crittografia di livello di crittografia. Assicurati che le chiavi private non vengano utilizzate da nessuna parte con il software server che supporta le connessioni SSLv2.

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Il servizio remoto supporta l'uso della cifratura RC4. L'host remoto supporta l'uso di RC4 in una o più suite di cifratura. Il cifrario RC4 è imperfetto nella sua generazione di un flusso di byte pseudo-casuale in modo che un'ampia varietà di piccoli pregiudizi venga introdotta nel flusso, diminuendo la sua casualità. Se il testo in chiaro viene crittografato ripetutamente (ad esempio, i cookie HTTP) e un utente malintenzionato è in grado di ottenere molti (cioè decine di milioni) di testi cifrati, l'attaccante potrebbe essere in grado di derivare il testo in chiaro.

Porta: 25

Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di crittografie RC4. Prendere in considerazione l'utilizzo di TLS 1.2 con le suite AES-GCM soggette al supporto del browser e del server Web.

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Vedi sopra

Porta: 5432

57582 - SSL Self-Signed Certificate

La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto. La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se il telecomando host è un host pubblico in produzione, questo annulla l'uso di SSL in quanto chiunque potrebbe stabilire un man-in-themiddle attacco contro l'host remoto. Si noti che questo plug-in non controlla le catene di certificati che terminano con un certificato non autofirmato, ma è firmato da un'autorità di certificazione non riconosciuta.

Porta: 25

Soluzione: Acquista o genera un certificato SSL appropriato per questo servizio.

57582 - SSL Self-Signed Certificate

Vedi sopra

Porta: 5432

26928 - SSL Weak Cipher Suites Supported

Il servizio remoto supporta l'uso di cifrari SSL deboli. L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia debole. Nota: questo è molto più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica.

Porta: 25

Soluzione: Riconfigurare l'applicazione interessata, se possibile per evitare l'uso di cifrari deboli.

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

L'host remoto supporta una serie di cifrari deboli. L'host remoto supporta le suite di cifratura EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un attaccante può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo. Un utente malintenzionato man-in-the-middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di crittografia EXPORT_RSA (ad es. CVE-2015-0204). Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

Porta: 25

Soluzione: Riconfigurare il servizio per rimuovere il supporto per le suite di cifratura EXPORT_RSA.

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

L'host remoto è affetto da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi cifrati utilizzando cifrari a blocchi in modalità Cipher Block Chaining (CBC). Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in appena 256 tentativi se sono in grado di forzare un'applicazione vittima ad inviare ripetutamente gli stessi dati su connessioni SSL 3.0 appena create. Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il "rollback" di una connessione a SSLv3, anche se TLSv1 o più recente è supportato dal client e dal servizio. Il meccanismo TLS Fallback SCSV impedisce gli attacchi di "rollback della versione" senza influire sui client legacy; tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non riescono a disabilitare SSLv3 immediatamente dovrebbero abilitare questo meccanismo. Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disabilitazione di SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

Porta: 25

Soluzione: Disabilita SSLv3. I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS fino a quando SSLv3 può essere disabilitato.

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

Vedi sopra

Porta: 5432

104743 - TLS Version 1.0 Protocol Detection

Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS. Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 ha difetti di progettazione nella crittografia. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero quindi essere usate quando possibile. A partire dal 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori. PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato completamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e i punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili ad alcuno exploit noti.

Porta: 25

Soluzione: Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.

104743 - TLS Version 1.0 Protocol Detection

Vedi sopra

Porta: 5432

VULNERABILITÀ MINORI:

70658 - SSH Server CBC Mode Ciphers Enabled

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Ciò può consentire a un utente malintenzionato per recuperare il messaggio in chiaro dal testo cifrato. Si noti che questo plug-in controlla solo le opzioni del server SSH e non verifica la vulnerabilità versioni del software.

Porta: 22

Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per disabilitare la crittografia della modalità CBC e abilitarla Crittografia in modalità cifratura CTR o GCM.

153953 - SSH Weak Key Exchange Algorithms Enabled

Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi deboli. Questo si basa sulla bozza del documento IETF “Key Exchange (KEX) Method Updates and Recommendations for Secure Shell” (SSH) draft-ietf-curdle-ssh-kex-sha2-20. La sezione 4 elenca le linee guida sugli algoritmi di scambio delle chiavi che NON DOVREBBE e NON DEVE essere abilitato.

Porta: 22

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

71049 - SSH Weak MAC Algorithms Enabled

Il server SSH remoto è configurato per consentire gli algoritmi MD5 e MAC a 96 bit. Il server SSH remoto è configurato per consentire gli algoritmi MD5 o MAC a 96 bit, entrambi considerati deboli.

Porta: 22

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

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

L'host remoto supporta le suite di cifratura EXPORT_DHE con chiavi inferiori o uguali a 512 bit. Attraverso crittoanalisi, una terza parte può trovare il segreto condiviso in un breve lasso di tempo. Un utente malintenzionato man-in-the-middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di crittografia EXPORT_DHE. Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

Porta: 25

Soluzione: Riconfigurare il servizio per rimuovere il supporto per le suite di cifratura EXPORT_DHE.

10407 - X Server Detection

Un server X11 è in ascolto sull'host remote. L'host remoto esegue un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto. Poiché il traffico X11 non è cifrato, è possibile che un utente malintenzionato intercetti la connessione.

Porta: 6000

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