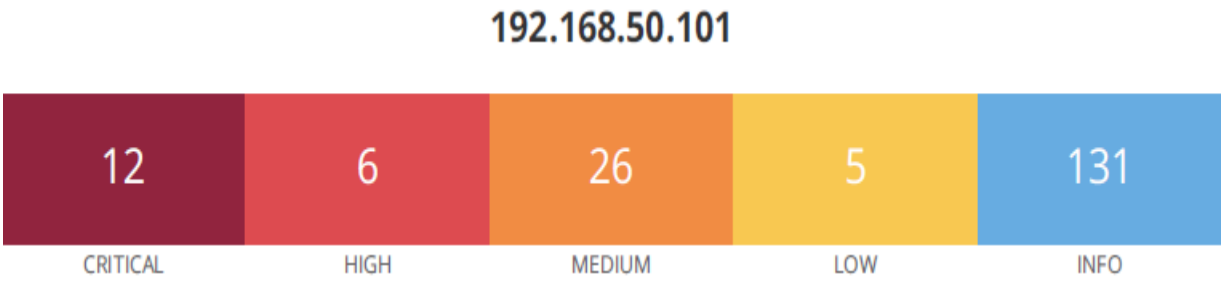
Alaimo Alessandro
24/11/2022

Vulnerability Assessment Tecnico



Informazioni sulla scansione

- Start time: Thu Nov 24 08:28:00 2022
- End time: Thu Nov 24 08:47:33 2022

Informazioni sull'host

- Netbios Name: METASPLOITABLE
- IP: 192.168.50.101
- MAC Address: 08:00:27:D2:25:45
- **OS: Linux Kernel 2.6 on Ubuntu 8.04**

Vulnerabilità Critiche

51988 - Bind Shell Backdoor Detection

Descrizione:

- Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla connettendosi alla porta remota e inviando direttamente i comandi.

Soluzione:

- Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Porta:

- tcp/1524/wild_shell

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descrizione:

- La chiave dell'host SSH remoto è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL. generatore di numeri casuali della libreria OpenSSL. Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e

utilizzarla per decifrare la sessione remota sessione remota o impostare un attacco man in the middle.

Soluzione:

- Considerate tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN devono essere rigenerati.

Porta:

- tcp/22/ssh

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

Descrizione:

- Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione:

- Considerate tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN devono essere rigenerati.

Porta:

- tcp/25/smtp

11356 - NFS Exported Share Information Disclosure

Descrizione:

- Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione:

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

Porta:

- udp/2049/rpc-nfs

20007 - SSL Version 2 and 3 Protocol Detection

Descrizione:

- Il servizio remoto accetta connessioni crittografate con SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono sono affette da diversi difetti crittografici, tra cui:
  - Uno schema di imbottitura insicuro con i cifrari CBC.
  - Schemi di rinegoziazione e ripresa della sessione non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client. tra il servizio interessato e i client. Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più alta del protocollo supportata (in modo che queste versioni vengano utilizzate solo se che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser web lo implementano in modo implementano questo metodo in modo non sicuro, consentendo a un aggressore di declassare una connessione (come nel caso di POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli. Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di di applicazione prevista da PCI DSS v3.1, qualsiasi versione di SSL non soddisfa la definizione di "crittografia forte" data da PCI SSC. crittografia forte".

Soluzione:

- Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare invece TLS 1.2 (con suite di cifratura approvate) o superiore.

Porta:

- tcp/25/smtp

33850 - Unix Operating System Unsupported Version Detection

Descrizione:

- Secondo il numero di versione dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione:

- Aggiornare a una versione del sistema operativo Unix attualmente supportata.

Porta:

- tcp/5432/postgresql

61708 - VNC Server 'password' Password

Descrizione:

- Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione:

- Proteggete il servizio VNC con una password forte.

10203 - rexecd Service Detection

Descrizione:

- Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è stato progettato per consentire agli utenti di una rete di eseguire comandi in remoto. Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi può essere abusato da un utente malintenzionato per eseguire la scansione di un host di terze parti.

Soluzione:

- Commentare la riga 'exec' in /etc/inetd.conf e riavviare il processo inetd.

Porta:

- tcp/0

Vulnerabilità Alte

10205 - rlogin Service Detection

Descrizione:

- Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile in quanto i dati vengono passati tra il client rlogin e il server in chiaro. Un aggressore man-in-the-middle può sfruttare questa situazione per sniffare login e password. password. Inoltre, può consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile Se l'host è vulnerabile all'indovinare il numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (compreso l'hijacking ARP su una rete locale), allora può essere possibile rete locale), allora potrebbe essere possibile bypassare l'autenticazione. Infine, rlogin è un modo semplice per trasformare l'accesso alla scrittura dei file in login completi attraverso i file .rhosts o rhosts.equiv.

Soluzione:

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

Porta:

- tcp/513/rlogin

34460 - Unsupported Web Server Detection

Descrizione:

- In base alla sua versione, il server Web remoto è obsoleto e non più gestito dal suo fornitore o provider. fornitore. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Soluzione:

- Rimuovere il server web se non è più necessario. Altrimenti, aggiornare a una versione supportata, se possibile, o passare a un altro server. passare a un altro server.

Porta:

- tcp/8180/www

61708 - VNC Server 'password' Password

Descrizione:

- Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione:

- Proteggete il servizio VNC con una password forte.

Porta:

- tcp/5900/vnc

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione:

- È stata riscontrata una vulnerabilità nella lettura/inclusione di file nel connettore AJP. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile. Nei casi in cui il server server vulnerabile consente l'upload di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file, ottenendo così un accesso remoto. una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione:

- Aggiornare 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, 9.0.31 o successivo.

Porta:

- tcp/8009/ajp13

Vulnerabilità Medie

136769 - ISC BIND Service Downgrade / Reflected DoS

Descrizione:

- Secondo la versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è affetta da vulnerabilità di downgrade delle prestazioni e DoS riflesso. Ciò è dovuto al fatto che BIND DNS non non limita sufficientemente il numero di fetch che possono essere eseguiti durante l'elaborazione di una risposta di rinvio. Un aggressore remoto non autenticato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come un server riflesso. utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

- Aggiornare alla versione di ISC BIND indicata nell'avviso del fornitore.

Porta:

- udp/53/dns

42256 - NFS Shares World Readable

Descrizione:

- Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base al nome host, all'IP, o intervallo IP).

Soluzione:

- Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

Porta:

- tcp/2049/rpc-nfs

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Descrizione:

- L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media forza. Nessus considera media forza qualsiasi crittografia che utilizzi chiavi di lunghezza pari ad almeno 64 bit e inferiore a 112 bit, oppure che utilizza la suite di crittografia 3DES. Si noti che è molto più facile aggirare la crittografia a media resistenza se l'aggressore si trova sulla stessa rete fisica.

Soluzione:

- Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari a media forza.

Porta:

- tcp/25/smtp

90509 - Samba Badlock Vulnerability

Descrizione:

- La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da una falla, nota come Badlock, che esiste nei protocolli SAM (Security Account Manager) e LSAD (Local Security Authority). (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali Remote Procedure Call (RPC). Procedure Remote (RPC). Un aggressore man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM. client e un server che ospita un database SAM può sfruttare questa falla per forzare il declassamento del livello di autenticazione, il che consente l'esecuzione di 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 di servizi critici. servizi critici.

Soluzione:

- Aggiornare a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Porta:

- tcp/445/cifs

12085 - Apache Tomcat Default Files

Descrizione:

- La pagina di errore predefinita, la pagina di indice predefinita, le JSP di esempio e/o le servlet di esempio sono installate sul server Apache Tomcat remoto. server Apache Tomcat remoto. Questi file devono essere rimossi perché potrebbero aiutare un utente malintenzionato a scoprire informazioni sull'installazione o sull'host Tomcat remoto.

Soluzione:

- Eliminate la pagina indice predefinita e rimuovete le JSP e le servlet di esempio. Seguire le istruzioni di Tomcat o OWASP per sostituire o modificare la pagina di errore predefinita.

Porta:

- tcp/8180/www

11213 - HTTP TRACE / TRACK Methods Allowed

Descrizione:

- Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni al server Web.

Soluzione:

- Disabilitare questi metodi HTTP. Per ulteriori informazioni, consultare l'output del plugin.

Porta:

- tcp/80/www

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

Descrizione:

- In base al numero di versione autodichiarato, l'installazione di ISC BIND in esecuzione sul server dei nomi remoto è la versione 9.x precedente alla 9.11.22, la 9.12.x precedente alla 9.16.6 o la 9.17.x precedente alla 9.17.4. Pertanto, è affetto da da una vulnerabilità di tipo denial of service (DoS) dovuta a un errore di asserzione durante il tentativo di verifica di una risposta troncata a una richiesta firmata TSIG. risposta a una richiesta firmata TSIG. Un utente autenticato e remoto può sfruttare questo problema inviando una risposta troncata a una richiesta firmata da TSIG. risposta troncata a una richiesta firmata TSIG per attivare un fallimento dell'asserzione, causando l'uscita del server. Si noti che Nessus non ha testato questo problema, ma si è basato solo sul numero di versione auto-riportato dell'applicazione. numero di versione dell'applicazione.

Soluzione:

- Aggiornare a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

Porta:

- udp/53/dns

136808 - ISC BIND Denial of Service

Descrizione:

- Esiste una vulnerabilità di tipo denial of service (DoS) nelle versioni di 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 utente remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente creato, per causare l'interruzione della risposta del servizio. Si noti che Nessus non ha testato questo problema, ma si è basato solo sul numero di versione auto-riportato dell'applicazione. numero di versione dell'applicazione.

Soluzione:

- Aggiornare alla release patchata più vicina alla versione attuale di BIND.

Porta:

- udp/53/dns

57608 - SMB Signing not required

Descrizione:

- La firma non è richiesta sul server SMB remoto. Un aggressore remoto non autenticato può sfruttare questa situazione per condurre attacchi man-in-the-middle contro il server SMB.

Soluzione:

- Applicare la firma dei messaggi nella configurazione dell'host. In Windows, questo si trova nell'impostazione di criterio 'Server di rete Microsoft: Firma digitale delle comunicazioni (sempre)". Su Samba, l'impostazione si chiama "server firma del server".

Porta:

- tcp/445/cifs

52611 - SMTP Service STARTTLS Plaintext Command Injection

Descrizione:

- Il servizio SMTP remoto contiene una falla software nella sua implementazione STARTTLS che potrebbe consentire a un aggressore remoto non autenticato di iniettare comandi durante la fase di protocollo plaintext che verranno eseguiti durante la fase di protocollo ciphertext. Uno sfruttamento riuscito potrebbe consentire a un aggressore di rubare l'e-mail della vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

Soluzione:

- Contattare il fornitore per verificare se è disponibile un aggiornamento.

Porta:

- tcp/25/smtp

90317 - SSH Weak Algorithms Supported

Descrizione:

- Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario Arcfour o nessun cifrario. o nessun cifrario. La RFC 4253 sconsiglia l'uso di Arcfour a causa di un problema di chiavi deboli.

Soluzione:

- Contattare il fornitore o consultare la documentazione del prodotto per rimuovere i cifrari deboli.

Porta:

- tcp/22/ssh

51192 - SSL Certificate Cannot Be Trusted

Descrizione:

- Il certificato X.509 del server non è attendibile. Questa situazione può verificarsi in tre modi diversi, in cui
- la catena di fiducia può essere interrotta, come indicato di seguito:
- - In primo luogo, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi sia quando il vertice della catena è un certificato non riconosciuto e autofirmato, sia quando mancano i certificati intermedi che collegherebbero il vertice della catena di certificati a un'autorità di certificazione pubblica nota.
- - In secondo luogo, la catena di certificati può contenere un certificato non valido al momento della scansione. Ciò può verificarsi sia quando la scansione avviene prima di una delle date "notBefore" del certificato, sia dopo una delle date "notAfter" del certificato. data "notAfter" del certificato.
- - In terzo luogo, la catena del certificato può contenere una firma che non corrisponde alle informazioni del certificato o che non può essere verificata. Le firme errate possono essere corrette facendo rifirmare il certificato con la firma errata dal suo emittente. Le firme che non possono essere verificate 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 della catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Questo potrebbe facilitare l'esecuzione di attacchi man-in-themiddle contro l'host remoto. contro l'host remoto.

Soluzione:

- Acquistare o generare un certificato SSL adeguato per questo servizio.

Porta:

- tcp/5432/postgresql

15901 - SSL Certificate Expiry

Descrizione:

- Questo plugin controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se sono già scaduti. e segnala se uno di essi è già scaduto.

Soluzione:

- Acquistare o generare un nuovo certificato SSL per sostituire quello esistente.

Porta:

- tcp/25/smtp

45411 - SSL Certificate with Wrong Hostname

Descrizione:

- L'attributo "commonName" (CN) del certificato SSL presentato per questo servizio è relativo a una macchina diversa.

Soluzione:

- Acquistare o generare un certificato SSL adeguato per questo servizio.

Porta:

- tcp/25/smtp

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

Descrizione:

- L'host remoto supporta SSLv2 e quindi potrebbe essere affetto da una vulnerabilità che permette un attacco cross-protocollo Bleichenbacher, noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità è dovuta a un difetto nell'implementazione di Secure Sockets Layer Version 2 (SSLv2). e consente di decifrare il traffico TLS catturato. Un attaccante man-in-the-middle può decifrare la connessione TLS utilizzando il traffico catturato in precedenza e una crittografia debole. insieme a una serie di connessioni appositamente create a un server SSLv2 che utilizza la stessa chiave privata.

Soluzione:

- Disattivare SSLv2 e le suite di crittografia di grado export. Assicurarsi che le chiavi private non vengano utilizzate con il software del server che supporta le connessioni SSLv2.

Porta:

- tcp/25/smtp

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Descrizione:

- L'host remoto supporta l'uso di RC4 in una o più suite di cifratura. Il cifrario RC4 ha un difetto nella generazione di un flusso pseudocasuale di byte, per cui un'ampia varietà di piccole distorsioni viene introdotta nel flusso, riducendone la casualità. di piccole distorsioni nel flusso, riducendo 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 (ad esempio, decine di milioni) testi cifrati, l'utente è in grado di ottenere un numero di milioni) di testi cifrati, l'aggressore potrebbe essere in grado di ricavare il testo in chiaro.

Soluzione:

- Se possibile, riconfigurare l'applicazione interessata per evitare l'uso dei cifrari RC4. Considerare l'utilizzo di TLS 1.2 con suite AES-GCM, a seconda del supporto del browser e del server web.

Porta:

- tcp/25/smtp

57582 - SSL Self-Signed Certificate

Descrizione:

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

Soluzione:

- Acquistare o generare un certificato SSL adeguato per questo servizio.

Porta:

- tcp/25/smtp

26928 - SSL Weak Cipher Suites Supported

Descrizione:

- 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.

Soluzione:

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

Porta:

- tcp/25/smtp

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

Descrizione:

- L'host remoto supporta le suite di cifratura EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato è in grado di determinare un modulo RSA a 512 bit in un breve lasso di tempo. Un utente malintenzionato potrebbe essere in grado di

declassare la sessione per utilizzare suite di cifratura EXPORT_RSA (ad es. CVE-2015-0204). Pertanto, si raccomanda di rimuovere il supporto per le suite di cifratura deboli.

Soluzione:

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

Porta:

- tcp/25/smtp

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

Descrizione:

- L'host remoto è affetto da una vulnerabilità di divulgazione di informazioni di tipo man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di padding durante la decodifica di messaggi crittografati con cifrari a blocchi in modalità CBC (cipher block chaining). Gli aggressori MitM possono decifrare un byte selezionato di un testo cifrato in appena 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente lo stesso testo cifrato. un'applicazione vittima a inviare ripetutamente gli stessi dati su connessioni SSL 3.0 appena create. Finché un client e un servizio supportano entrambi SSLv3, una connessione può essere "riportata" a SSLv3, anche se TLSv1 o più recente è supportato dal client. Il meccanismo TLS Fallback SCSV previene gli attacchi "version rollback" senza impattare i client legacy; Tuttavia, può proteggere le connessioni solo se il client e il servizio supportano il meccanismo. I siti che non possono disabilitare immediatamente SSLv3 dovrebbero abilitare questo meccanismo. Si tratta di una vulnerabilità della specifica SSLv3, non di una particolare implementazione SSL. La disabilitazione di SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

Soluzione:

- Disabilitare SSLv3.
  I servizi che devono supportare SSLv3 devono abilitare il meccanismo TLS Fallback SCSV fino a quando non sarà possibile disabilitare SSLv3.

Porta:

- tcp/25/smtp

104743 - TLS Version 1.0 Protocol Detection

Descrizione:

- Il servizio remoto accetta connessioni criptate con TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 attenuano questi problemi, ma le versioni più recenti di TLS, come la 1.2 e la 1.3, sono

progettate contro questi difetti e dovrebbero essere utilizzate ogni volta che è possibile. A partire dal 31 marzo 2020, gli endpoint che non sono 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 completamente disabilitato entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti terminali SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili di exploit noti. exploit noti.

Soluzione:

- Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.

Porta:

- tcp/25/smtp

42263 - Unencrypted Telnet Server

Descrizione:

- L'host remoto sta eseguendo un server Telnet su un canale non criptato. L'uso di Telnet su un canale non crittografato è sconsigliato, poiché login, password e comandi vengono trasferiti in chiaro. Ciò consente a un aggressore remoto, man-in-the-middle, di origliare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e di modificare il traffico scambiato tra client e server. SSH è preferibile a Telnet perché protegge le credenziali dalle intercettazioni e può convogliare altri flussi di dati, come ad esempio X11. flussi di dati aggiuntivi, come una sessione X11.

Soluzione:

- Disattivare il servizio Telnet e utilizzare invece SSH.

Porta:

- tcp/23/telnet

Vulnerabilità Basse

31705 - SSL Anonymous Cipher Suites Supported

Descrizione:

- L'host remoto supporta l'uso di cifrari SSL anonimi. Se da un lato questo consente all'amministratore di impostare un servizio che cripta il traffico senza dover generare e configurare certificati SSL, dall'altro 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.

Soluzione:

- Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari deboli.

Porta:

- tcp/25/smtp

70658 - SSH Server CBC Mode Ciphers Enabled

Descrizione:

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

Soluzione:

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

Porta:

- tcp/22/ssh

153953 - SSH Weak Key Exchange Algorithms Enabled

Descrizione:

- Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi considerati 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 indicazioni sugli algoritmi di scambio di chiavi che NON DEVONO e NON devono essere abilitati. Questo include:
  diffie-hellman-gruppo-scambio-sha1
  diffie-hellman-gruppo1-sha1
  gss-gex-sha1-*
  gss-gruppo1-sha1-*
  gss-gruppo14-sha1-*
  rsa1024-sha1
  Si noti che questo plugin controlla solo le opzioni del server SSH e non controlla le versioni vulnerabili del software. versioni del software.

Soluzione:

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

Porta:

- tcp/22/ssh

71049 - SSH Weak MAC Algorithms Enabled

Descrizione:

- Il server SSH remoto è configurato per consentire gli algoritmi MD5 o MAC a 96 bit, entrambi considerati deboli. Si noti che questo plugin controlla solo le opzioni del server SSH e non

controlla le versioni vulnerabili del software. versioni software vulnerabili.

Soluzione:

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

Porta:

- tcp/22/ssh

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

Descrizione:

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

Soluzione:

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

Porta:

- tcp/25/smtp

10407 - X Server Detection

Descrizione:

- L'host remoto sta eseguendo un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare le applicazioni grafiche applicazioni grafiche in esecuzione su un determinato host su un client remoto. Poiché il traffico X11 non è cifrato, un utente malintenzionato può intercettare la connessione.

Soluzione:

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

Porta:

- tcp/6000/x11