Claudio De cicco
24/11/2022

Report Tecnico Vulnerabilità (192.168.1.102)

13	6	26	5	132
CRITICAL	HIGH	MEDIUM	LOW	INFO

METASPLOITABLE
IP:192.168.1.102
MAC Address:08:00:27:F0:63:36
OS:Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

In seguito verranno riportate nel dettaglio tutte le vulnerabilità dalla piu' critica a quelle meno rilevanti.

CRITICAL

-134862 Apache Tomcat A JP Connector Request Injection (Ghostcat)
C'è un connettore AJP vulnerabile in ascolto sull'host.
Soluzione : Aggiorna la configurazione A JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51,9.0.31 o successivo.

-**51988** Bind Shell Backdoor Detection
L'host remoto potrebbe essere stato compromesso. Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato potrebbe utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.
Soluzione : Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

-**32314** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Le chiavi SSH dell'host remoto sono deboli. La chiave è stata generata su un sistema Debian o Ubuntu che contiene un bug nel file generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota diOpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione del telecomando sessione o impostare un attacco man in the middle.
Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto, in particolare tutto il materiale SSH,Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

-**32321** - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Il certificato SSL remoto utilizza una chiave debole. 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 a un packager Debian che rimuove 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 o impostare un attacco man in the middle.
Soluzione: Considerare indovinabile tutto il materiale crittografico generato sull'host remoto, in particolare tutto il materiale SSH,Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

-**11356** NFS Exported Share Information Disclosure
È possibile accedere alle condivisioni NFS sull'host remoto.Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione.L'attaccante potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.
Soluzione: Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

-**20007** SSL Version 2 and 3 Protocol Detection
Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0 Queste versioni di SSL sonoaffetto da diversi difetti crittografici, tra cui:
- Uno schema di riempimento insicuro con cifrari CBC.
- Schemi di rinegoziazione e ripresa delle sessioni non sicure.
Un utente malintenzionato può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i clienti.Sebbene SSL/TLS abbia un mezzo sicuro per scegliere la versione più supportata del protocollo (es che queste versioni verranno utilizzate solo se il client o il server non supportano niente di meglio), molti browser web implementarlo in un modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione (come in POODLE).Pertanto, si consiglia di disabilitare completamente questi protocolli.
Soluzione: Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare invece TLS 1.2 (con pacchetti di crittografia approvati) o versioni successive.

-**33850** Unix Operating System Unsupported Version Detection
Il sistema operativo in esecuzione sull'host remoto non è più supportato. il sistema operativo Unix in esecuzione sull'host remoto è non più supportato.La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto di conseguenza, è probabile che contenga vulnerabilità di sicurezza.
Soluzione: Aggiorna a una versione del sistema operativo Unix attualmente supportata

-**46882** UnrealIRCd Backdoor Detection
Il server IRC remoto contiene una backdoor.Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire Codice arbitrario sull'host interessato.
Soluzione: Scarica nuovamente il software, verificalo utilizzando i checksum MD5/SHA1 pubblicati e reinstallalo

-**34460** Unsupported Web Server Detection
Il server Web remoto è obsoleto/non supportato.Secondo la sua versione, il server Web remoto è obsoleto e non è più mantenuto dal suo fornitore o fornitore.La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto di conseguenza, potrebbe contenere vulnerabilità di sicurezza.
Soluzione: Rimuovi il server Web se non è più necessario.In caso contrario, aggiorna a una versione supportata se possibile o passare a un altro server.

-**61708** VNC Server 'password' Password
Un server VNC in esecuzione sull'host remoto è protetto da una password debole.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 di 'password'.Un utente malintenzionato remoto e non autenticato potrebbe sfruttarequesto per prendere il controllo del sistema.
Soluzione: Proteggi il servizio VNC con una password sicura.

-**10203** rexecd Service Detection
Il servizio rexecd è in esecuzione sull'host remoto ed è progettato per consentire agli utenti di una rete di farlo eseguire i comandi da remoto.Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi potrebbe essere abusato da un utente malintenzionato per eseguire la scansione di un host di terze parti.
Soluzione: Commenta la riga 'exec' in /etc/inetd.conf e riavvia il processo inetd

HIGH

- **136769** - ISC BIND Service Downgrade / Reflected DoS
Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessato dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse.Ciò è dovuto al fatto che BIND DNS non riesce a limitare sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di rinvio.Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o utilizzare il server interessato come riflettore in un attacco di riflessione.
Soluzione: Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.

- **42256** NFS Shares World Readable
Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP,o intervallo IP).
Soluzione: Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

- **42873** SSL Medium Strength Cipher Suites Supported (SWEET32)
L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di livello medio. Nessus riguarda forza media come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizza la suite di crittografia 3DES. Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sullo stesso rete fisica.
Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature di livello medio.

- **90509** Samba Badlock Vulnerability
La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è interessata da un difetto, noto come Badlock, che esiste nel Security Account Manager (SAM) e nell'autorità di sicurezza locale (Domain Policy) (LSAD) a causa di una negoziazione errata del livello di autenticazione su procedura remota Canali di chiamata (RPC): un attaccante man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM possono sfruttare questo difetto per forzare un downgrade dell'autenticazione livello, 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.
Soluzione: Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

- **10205** rlogin Service Detection
Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono scambiati tra di loro il client e il server rlogin in chiaro. Un attaccante man-in-the-middle può sfruttarlo per sniffare accessi e password.Inoltre, può consentire accessi scarsamente autenticati senza password.Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su un local rete) allora potrebbe essere possibile bypassare l'autenticazione.Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura ai file in accessi completi tramite i file .rhosts o rhosts.equiv.
Soluzione: Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo service e utilizzare invece SSH.

MEDIUM

- **12085** Apache Tomcat Default Files
Il server Web remoto contiene file predefiniti.La pagina di errore predefinita, la pagina indice predefinita, i JSP di esempio e/o i servlet di esempio sono installati su server Apache Tomcat remoto. Questi file dovrebbero essere rimossi in quanto potrebbero aiutare un utente malintenzionato a scoprirli informazioni sull'installazione remota di Tomcat o sull'host stesso.
Soluzione: Elimina la pagina indice predefinita e rimuovi JSP e servlet di esempio.Segui Tomcat o OWASP istruzioni per sostituire o modificare la pagina di errore predefinita.

- **11213** HTTP TRACE / TRACK Methods Allowed
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.
Soluzione: Disattiva questi metodi HTTP. Per ulteriori informazioni, fai riferimento all'output del plug-in

- **139915** ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
Il server dei nomi remoto è affetto da una vulnerabilità Denial of Service.
In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul nome remoto server è la versione 9.x precedente alla 9.11.22, 9.12.x precedente alla 9.16.6 o 9.17.x precedente alla 9.17.4.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 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.Si noti che Nessus non ha testato questo problema, ma si è invece affidato solo alle auto-segnalazioni dell'applicazionenumero della versione.
Soluzione: Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo

- **136808** ISC BIND Denial of Service
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 versioni precedenti. Un utente malintenzionato remoto non autenticato può sfruttare questo problema,tramite un messaggio appositamente predisposto, per impedire al servizio di rispondere.Si noti che Nessus non ha testato questo problema, ma si è invece affidato solo alle auto-segnalazioni dell'applicazione numero della versione.
Soluzione: Aggiorna alla versione con patch più strettamente correlata 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 utente malintenzionato remoto non autenticato può sfruttare questa opzione per. condurre attacchi man-in-the-middle contro il server SMB.
Soluzione: Applica la firma dei messaggi nella configurazione dell'host. In Windows, questo si trova nell'impostazione dei criteri 'Server di rete Microsoft: firma digitale delle comunicazioni (sempre)'. Su Samba, l'impostazione si chiama 'server' firma'. Vedere il 'vedi anche' collegamenti per ulteriori dettagli.

- **52611** SMTP Service STARTTLS Plaintext Command Injection
Il servizio di posta remota consente l'iniezione di comandi in chiaro durante la negoziazione di un canale di comunicazione.Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire un remoto, attaccante non autenticato per iniettare i comandi durante la fase di protocollo in chiaro che sarà eseguito durante la fase del protocollo ciphertext.Lo sfruttamento di successo potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o SASL associato (Semplice Credenziali di autenticazione e livello di sicurezza).
Soluzione: Contatta il fornitore per vedere se è disponibile un aggiornamento**.**

- **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 il cifrario flusso Arcfour o no cifratura a tutti. RFC 4253 sconsiglia di utilizzare Arcfour a causa di un problema con le chiavi deboli.
Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per rimuovere i cifrari deboli

- **31705** SSL Anonymous Cipher Suites Supported
L'host remoto supporta l'uso di cifrari SSL anonimi. Mentre questo consente a un amministratore di impostare 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 rendere il servizio vulnerabile ad un attacco man-in-the-middle. Nota: Questo è molto più facile da sfruttare se l'attaccante è sulla stessa rete fisica.
Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari deboli.

- **51192** SSL Certificate Cannot Be Trusted
Il certificato X.509 del server non può essere considerato 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 provenire da un pubblico noto
autorità di certificazione. Questo può verificarsi sia quando la parte superiore della catena è un non riconosciuto, auto-firmato
certificato, o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati
a una nota autorità pubblica di certificazione.
- In secondo luogo, la catena di certificati può contenere un certificato non valido al momento della scansione. Questo può
si verifica quando la scansione avviene prima di una delle date 'notbefore' del certificato, o dopo una delle
Le date del certificato non sono aggiornate.
- In terzo luogo, la catena del certificato può contenere una firma che non corrisponde alle informazioni del certificato
o non può essere verificato. Le firme errate possono essere corrette ottenendo il certificato con la firma errata
ri-firmato dal suo emittente. Firme che non possono essere verificate sono il risultato dell'emittente del certificato utilizzando un
firma algoritmo 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
per verificare l'autenticità e l'identità del server web. Questo potrebbe rendere più facile effettuare attacchi man-in-the-middle contro l'host remoto.
Soluzione: Acquistare o generare un certificato SSL appropriato per questo servizio.

- **15901** - SSL Certificate Expiry
Questo plugin controlla le date di scadenza dei certificati associati con SSL- servizi abilitati sulla destinazione e segnala se ne sono già scaduti.
Soluzione: Acquistare o generare un nuovo certificato SSL per sostituire quello esistente.

- **45411** - SSL Certificate with Wrong Hostname
L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa.
Soluzione: Acquistare o generare un certificato SSL appropriato per questo servizio

- **89058** - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
L'host remoto supporta SSLv2 e quindi può essere interessato da una vulnerabilità che consente un protocollo incrociato Bleichenbacher padding oracolo attacco noto come DROWN (Decriptare RSA con obsoleto e Crittografia indebolita). Questa vulnerabilità esiste a causa di un difetto nel livello Secure Sockets versione 2 (SSLv2) implementazione, e permette di catturare il traffico TLS da decifrare. Un uomo-in-the-middle attaccante può sfruttare questo per decifrare la connessione TLS utilizzando traffico precedentemente catturato e crittografia debole insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.
Soluzione: Disabilita le suite di cifratura SSLv2 ed export grade. Assicurati che le chiavi private non siano usate da nessuna parte con software server che supporta connessioni SSLv2.

- **65821 -** SSL RC4 Cipher Suites Supported (Bar Mitzvah)
L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.Il cifrario RC4 è difettoso nella sua generazione di un flusso pseudo-casuale di byte in modo che una grande varietà di piccoli pregiudizi vengono introdotti nel flusso, diminuendo la sua casualità.Se il testo in chiaro è ripetutamente crittografato (ad esempio, i cookie HTTP), e un utente malintenzionato è in grado di ottenere molti (cioè, decine di milioni) testi cifrati, l'attaccante può essere in grado di derivare il testo in chiaro.
Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari RC4. Considerare l'uso di TLS 1.2 con Suite AES-GCM soggette al supporto di browser e server web.

- **57582 -** SSL Self-Signed Certificate
La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host è un host pubblico in produzione, questo annulla l'uso di SSL come chiunque potrebbe stabilire un man-in-the attacco medio contro l'host remoto.Si noti che questo plugin non controlla le catene di certificati che terminano in un certificato che non è autofirmato, ma è firmato da un'autorità di certificazione non riconosciuta.
Soluzione: Acquistare o generare un certificato SSL appropriato per questo servizio.

- **26928** - SSL Weak Cipher Suites Supported
L'host remoto supporta l'uso di cifrari SSL che offrono crittografia debole.
Nota: Questo è molto più facile da sfruttare se l'attaccante è sulla stessa rete fisica.
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 le suite di cifratura EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un attaccante può calcolare un modulo RSA a 512 bit in un breve lasso di tempo.Un attaccante man-in-the middle può essere in grado di declassare la sessione per usare le suite di cifratura EXPORT_RSA (es.CVE-2015-0204). Quindi, si consiglia di rimuovere il supporto per suite di cifratura deboli.
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 interessato da un man-in-the-middle (MitM) vulnerabilità divulgazione delle informazioni noto come BARBONCINO. La vulnerabilità è dovuta al modo SSL 3.0 gestisce i byte di riempimento quando decifrare i messaggi cifrato usando 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 per inviare ripetutamente gli stessi dati sulle connessioni SSL 3.0 appena create.Finché un client e un servizio supportano entrambi SSLv3, una connessione può essere 'rollback' a SSLv3, anche se TLSv1 o più recente è supportato dal client e dal servizio.Il meccanismo TLS Fallback SCSV previene gli attacchi di rollback delle versioni senza impattare sui client legacy;tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. Siti cheimpossibile disabilitare SSLv3 immediatamente dovrebbe attivare questo meccanismo.Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. Disabilitare SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.
Soluzione: Disattivare SSLv3.I servizi che devono supportare SSLv3 dovrebbero abilitare il meccanismo TLS Fallback SCSV fino a quando SSLv3 può essere disabilitato.

- **104743** - TLS Version 1.0 Protocol Detection
Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0. TLS 1.0 ha un numero di crittografia difetti di progettazione. implementazioni moderne di TLS 1.0 mitigare questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettati contro questi difetti e dovrebbero essere utilizzati quando possibile.Al 31 marzo 2020, gli endpoint non abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser web e fornitori principali. PCI DSS v3.2 richiede che TLS 1.0 sia disabilitato interamente entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e i punti terminali SSL/TLS a cui si collegano) che possono essere verificati come non suscettibili diimprese conosciute.
Soluzione: Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.

- **42263** - Unencrypted Telnet Server
L'host remoto esegue un server Telnet su un canale non crittografato.L'utilizzo di Telnet su un canale non crittografato non è raccomandato in quanto i login, le password e i comandi sono trasferito in chiaro. Questo permette a un attaccante remoto, man-in-the-middle di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e per modificare il traffico scambiato tra un client e server.SSH è preferito rispetto Telnet in quanto protegge le credenziali da intercettazioni e può tunnel aggiuntivo flussi di dati come una sessione X11.
Soluzione: Disabilitare il servizio Telnet e usare invece SSH.

LOW

- **70658** - SSH Server CBC Mode Ciphers Enabled
Il server SSH è configurato per supportare la crittografia CBC (Cipher Block Chaining). Ciò potrebbe consentire un attaccante per recuperare il messaggio in chiaro dal testo cifrato.Si noti che questo plugin controlla solo le opzioni del server SSH e non controlla per vulnerabiliversioni software.
Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per disattivare la crittografia cifratura in modalità CBC e abilitareCifratura CTR o GCM.

- **153953** - SSH Weak Key Exchange Algorithms Enabled
Il server SSH remoto è configurato per consentire algoritmi di scambio chiavi considerati deboli. Questo si basa sulla bozza di documento IETF Key Exchange (KEX) Metodo Aggiornamenti e raccomandazioni per Secure Shell (SSH) draft-ietf-curdle-ssh-kex-Sha2-20.
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 algoritmi MD5 o MAC a 96 bit, entrambi considerato debole.Si noti che questo plugin controlla solo le opzioni del server SSH, e non controlla per vulnerabili versioni software.
Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MD5 e MAC a 96 bit.

- **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 crittanalisi, una terza parte può trovare il segreto condiviso in un breve lasso di tempo. Un attaccante man-in-the medio potrebbe essere in grado di declassare la sessione per usare 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

- **10407** - X Server Detection
L'host remoto sta eseguendo un server X11. X11 è un protocollo client-server che può essere usato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto. Dal momento che il traffico X11 non è cifrato, è possibile per un attaccante di intercettare la connessione.
Soluzione: Limita l'accesso a questa porta. Se la funzione client/server X11 non è usata, disabilita completamente il supporto TCP in X11 (-nolisten tcp).