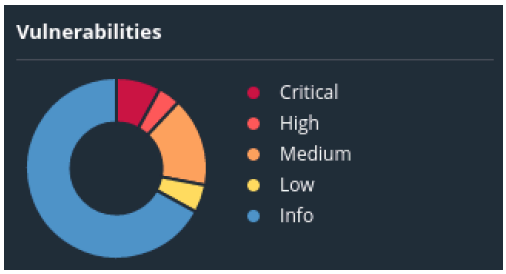
4. Assessment delle vulnerabilità

Vulnerability Assessment con Nessus sulla macchina Metasploitable
(Scansione delle porte comuni)

REPORT DIRIGENZIALE



192.168.50.101

10	5	24	5	124
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Feb 23 13:06:24 2023
End time:	Thu Feb 23 13:32:50 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	5E:3D:A7:78:8B:81
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

GRAVITA SCORE NOME

CRITICAL 9.8 Apache Tomcat A JP Connector Request Injection (Ghostcat)
C'è un connettore A JP vulnerabile in ascolto sull'host remoto.

CRITICAL 9.8 Bind Shell Backdoor Detection
L'host remoto potrebbe essere stato compromesso.

CRITICAL 9.8 SSL Version 2 and 3 Protocol Detection
Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

CRITICAL 10.0 Unix Operating System Unsupported Version Detection
Il sistema operativo in esecuzione sull'host remoto non è più supportato.

CRITICAL 10.0* Debian OpenSSH/OpenSSL Package Random Number GeneratorWeakness
Le chiavi dell'host SSH remoto sono deboli

CRITICAL 10.0* Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Il certificato SSL remoto utilizza una chiave debole.

CRITICAL 10.0* NFS Exported Share Information Disclosure
È possibile accedere alle condivisioni NFS sull'host remoto.

CRITICAL 10.0* VNC Server 'password' Password
Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

HIGH 8.6 ISC BIND Service Downgrade / Reflected DoS
Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.

HIGH 7.5 NFS Shares World Readable
Il server NFS remoto esporta condivisioni leggibili da tutti.8 >

HIGH 7.5 SSL Medium Strength Cipher Suites Supported (SWEET32)
Il servizio remoto supporta l'uso di crittografie SSL di livello medio.

HIGH 7.5 Samba Badlock Vulnerability
Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

MEDIUM 6.8 SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
È possibile ottenere informazioni riservate dall'host remoto con servizi abilitati per SSL/TLS.

MEDIUM 6.5 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.

MEDIUM 6.5 SSL Certificate Cannot Be Trusted
Il certificato SSL per questo servizio non può essere attendibile.

MEDIUM 6.5 SSL Self-Signed Certificate
La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto.

MEDIUM 6.5 TLS Version 1.0 Protocol Detection
Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.

MEDIUM 5.9 ISC BIND Denial of Service
Il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione.

MEDIUM 5.9 SSL Anonymous Cipher Suites Supported
Il servizio remoto supporta l'uso di cifrari SSL anonimi.

MEDIUM 5.9 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
traffico TLS acquisito.

MEDIUM 5.9 SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Il servizio remoto supporta l'uso della cifratura RC4.

MEDIUM 5.3 HTTP TRACE / TRACK Methods Allowed
Le funzioni di debug sono abilitate sul server Web remoto.

MEDIUM 5.3 SMB Signing not required
La firma non è richiesta sul server SMB remoto.

MEDIUM 5.3 SSL Certificate Expiry
Il certificato SSL del server remoto è già scaduto.

MEDIUM 5.3 SSL Certificate with Wrong Hostname
Il certificato SSL per questo servizio è per un host diverso.

MEDIUM 5.3 SSL Weak Cipher Suites Supported
Il servizio remoto supporta l'uso di cifrari SSL deboli.

MEDIUM 4.0* SMTP Service STARTTLS Plaintext Command Injection
Il servizio di posta remota consente l'iniezione di comandi in testo normale durante la negoziazione di un file crittografato
canale di comunicazione.

MEDIUM 4.3* SSH Weak Algorithms Supported
Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo.

MEDIUM 4.3* SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
L'host remoto supporta una serie di cifrari deboli.

LOW 3.7 SSH Weak Key Exchange Algorithms Enabled
Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi deboli.

LOW 3.7 SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
L'host remoto supporta una serie di cifrari deboli.

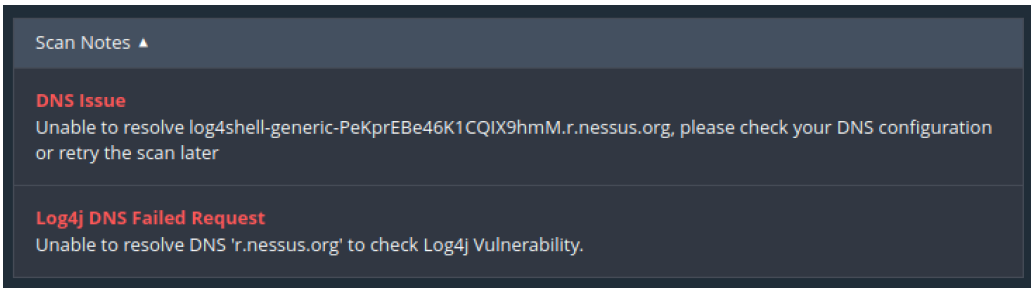
LOW 2.6* SSH Server CBC Mode Ciphers Enabled
Il server SSH è configurato per utilizzare Cipher Block Chaining.

LOW 2.6* SSH Weak MAC Algorithms Enabled
Il server SSH remoto è configurato per consentire gli algoritmi MD5 e MAC a 96 bit.

LOW 2.6* X Server Detection
Un server X11 è in ascolto sull'host remoto

Abbiamo poi riscontrato la presenza di Info Vulnerabilities (124) i quali non hanno un fattore di rischio, ma che sono Tati comunque riportati nel grafico sopra.

Scan Notes



REPORT TECNICO

192.168.50.101

Scan Information

Start time:	Thu Feb 23 13:06:24 2023
End time:	Thu Feb 23 13:32:50 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
MAC Address:	5E:3D:A7:78:8B:81
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

GRAVITA	SCORE	NOME
CRITICAL	9.8	Apache Tomcat A JP Connector Request Injection (Ghostcat)

C'è un connettore A JP vulnerabile in ascolto sull'host remoto.

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Potrebbe farlo un utente malintenzionato remoto e non autenticato
sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il
server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno
una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

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.

CRITICAL	9.8	Bind Shell Backdoor Detection

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarlo da

collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione

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

CRITICAL 9.8 SSL Version 2 and 3 Protocol Detection

Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono
affetto 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.
Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di
applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di PCI SSC di "forte
crittografia'.

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.

CRITICAL 10.0 Unix Operating System Unsupported Version Detection

Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione

Secondo il suo numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto è no
più supportato.
La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Come un
risultato, è probabile che contenga vulnerabilità di sicurezza.

Soluzione

Aggiorna a una versione del sistema operativo Unix attualmente supportata.

CRITICAL 10.0* Debian OpenSSH/OpenSSL Package Random Number GeneratorWeakness

Le chiavi dell'host SSH remoto sono deboli

Descrizione

La chiave dell'host SSH remoto 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 di
OpenSSL.
Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione del telecomando
sessione o impostare un uomo nel mezzo dell'attacco.

Soluzione

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH,
Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

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

Il certificato SSL remoto utilizza una chiave debole.

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 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 uomo nel mezzo dell'attacco.

Soluzione

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH,
Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

CRITICAL 10.0* NFS Exported Share Information Disclosure

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. UN
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.

CRITICAL 10.0* VNC Server 'password' Password

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

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 di 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare
questo per prendere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password complessa.

HIGH 8.6 ISC BIND Service Downgrade / Reflected DoS

Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.

Descrizione

Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto
è influenzato dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto a BIND DNS no
limitando 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.

HIGH 7.5 NFS Shares World Readable

Il server NFS remoto esporta condivisioni leggibili da tutti.8 >

Descrizione

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.

HIGH 7.5 SSL Medium Strength Cipher Suites Supported (SWEET32)

Il servizio remoto supporta l'uso di crittografie SSL di livello medio.

Descrizione

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nesso saluta
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.

HIGH 7.5 Samba Badlock Vulnerability

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Descrizione

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 a
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.

MEDIUM 6.8 SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

È possibile ottenere informazioni riservate dall'host remoto con servizi abilitati per SSL/TLS.

Descrizione

L'host remoto è affetto da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come
BARBONCINO. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi
crittografato 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 per 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. Siti che
Impossibile disabilitare SSLv3 immediatamente dovrebbe 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.

Soluzione

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

MEDIUM 6.5 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.

Descrizione

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. 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.
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 a BIND 9.11.22, 9.16.6, 9.17.4 o successivo

MEDIUM 6.5 SSL Certificate Cannot Be Trusted

Il certificato SSL per questo servizio non può essere attendibile.

Descrizione

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:
- In primo luogo, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un pubblico noto
autorità di certificazione. 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. Questo può
verificarsi quando la scansione avviene prima di una delle date 'notBefore' del certificato o dopo una delle date
le date "notAfter" del certificato.
- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrispondeva alle informazioni del certificato
o non è stato possibile verificarlo. Le firme errate possono essere corrette ottenendo il certificato con la firma errata
nuovamente firmato dal suo emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato a
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 le cose più difficili per gli utenti
per verificare l'autenticità e l'identità del server web. Questo potrebbe rendere più facile l'esecuzione di man-in-the-
attacchi medi contro l'host remoto.

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

MEDIUM 6.5 SSL Self-Signed Certificate

La catena di certificati SSL per questo servizio termina con un certificato autofirmato non riconosciuto.

Descrizione
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 uomo-in-the-
attacco medio 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.

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

MEDIUM 6.5 TLS Version 1.0 Protocol Detection

Il servizio remoto crittografa il traffico utilizzando una versione precedente di TLS.

Descrizione
Il servizio remoto accetta connessioni crittografate tramite TLS 1.0. TLS 1.0 ha un numero di crittografia
difetti di progettazione. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS sono simili
1.2 e 1.3 sono progettati contro questi difetti e dovrebbero essere usati 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.

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

MEDIUM 5.9 ISC BIND Denial of Service

Il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione.

Descrizione

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 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.

MEDIUM 5.9 SSL Anonymous Cipher Suites Supported

Il servizio remoto supporta l'uso di cifrari SSL anonimi.

Descrizione

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 farlo
verifica 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

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

MEDIUM 5.9 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
traffico TLS acquisito.

Descrizione

L'host remoto supporta SSLv2 e pertanto potrebbe essere interessato da una vulnerabilità che consente un cross-
protocollo Bleichenbacher padding oracle attacco noto come DROWN (Decrypting RSA with Obsolete and

crittografia indebolita). Questa vulnerabilità esiste a causa di un difetto nel Secure Sockets Layer Version 2 (SSLv2)
implementazione e consente di decrittografare il traffico TLS acquisito. Un attaccante man-in-the-middle può farlo
sfruttalo per decrittografare la connessione TLS utilizzando il traffico acquisito in precedenza e la crittografia debole
insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.

Soluzione

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

MEDIUM 5.9 SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Il servizio remoto supporta l'uso della cifratura RC4.

Descrizione

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 vengono introdotti nel flusso, diminuendo la sua casualità.
Se il testo in chiaro viene crittografato ripetutamente (ad es. cookie HTTP) e un utente malintenzionato è in grado di ottenerne molti (ovvero decine di
milioni) di testi cifrati, l'aggressore potrebbe essere in grado di ricavare il testo in chiaro.

Soluzione

Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di crittografie RC4. Prendi in considerazione l'utilizzo di TLS 1.2 con
Suite AES-GCM soggette al supporto di browser e server web.

MEDIUM 5.3 HTTP TRACE / TRACK Methods Allowed

Le funzioni di debug sono abilitate sul server Web remoto.

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 del server Web.

Soluzione

Disattiva questi metodi HTTP. Fare riferimento all'output del plug-in per ulteriori informazioni.

MEDIUM 5.3 SMB Signing not required

La firma non è richiesta sul server SMB remoto.

Descrizione

La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttarlo per
condurre attacchi man-in-the-middle contro il server SMB.

Soluzione

Imponi 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'. Vedere i collegamenti "vedi anche" per ulteriori dettagli.

MEDIUM 5.3 SSL Certificate Expiry

Il certificato SSL del server remoto è già scaduto.

Descrizione

Questo plug-in controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e
segnala se qualcuno è già scaduto.

Soluzione

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

MEDIUM 5.3 SSL Certificate with Wrong Hostname

Il certificato SSL per questo servizio è per un host diverso.

Descrizione

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

Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

MEDIUM 5.3 SSL Weak Cipher Suites Supported

Il servizio remoto supporta l'uso di cifrari SSL deboli.

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.

MEDIUM 4.0* SMTP Service STARTTLS Plaintext Command Injection

Il servizio di posta remota consente l'iniezione di comandi in testo normale durante la negoziazione di un file crittografato
canale di comunicazione.

Descrizione

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a
utente malintenzionato remoto e non autenticato per iniettare comandi durante la fase del protocollo in chiaro che sarà
eseguito durante la fase del protocollo del testo cifrato.
Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o SASL (Simple
credenziali di autenticazione e livello di sicurezza).

Soluzione

Contattare il fornitore per vedere se è disponibile un aggiornamento.

MEDIUM 4.3* SSH Weak Algorithms Supported

Il server SSH remoto è configurato per consentire algoritmi di crittografia deboli o nessun algoritmo.

Descrizione

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario a flusso Arcfour o no
cifrare affatto. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con chiavi deboli.

Soluzione

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

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

L'host remoto supporta una serie di cifrari deboli.

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

LOW 3.7 SSH Weak Key Exchange Algorithms Enabled

Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi deboli.
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 linee guida sugli algoritmi di scambio delle chiavi
che NON DEVE e NON DEVE essere abilitato. Ciò comprende:
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
gss-gex-sha1-*
gss-group1-sha1-*
gss-group14-sha1-*
rsa1024-sha1
Si noti che questo plug-in controlla solo le opzioni del server SSH e non verifica la vulnerabilità
versioni del software.
Solution
Contact the vendor or consult product documentation to disable the weak algorithms.

LOW 3.7 SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

L'host remoto supporta una serie di cifrari deboli.
Descrizione
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.

Soluzione

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

LOW 2.6* SSH Server CBC Mode Ciphers Enabled

Il server SSH è configurato per utilizzare Cipher Block Chaining.

Descrizione

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.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable
CTR or GCM cipher mode encryption.

LOW 2.6* SSH Weak MAC Algorithms Enabled

Il server SSH remoto è configurato per consentire gli algoritmi MD5 e MAC a 96 bit.

Descrizione

Il server SSH remoto è configurato per consentire gli algoritmi MD5 o MAC a 96 bit, entrambi disponibili
considerato debole.
Si noti che questo plug-in controlla solo le opzioni del server SSH e non verifica la vulnerabilità
versioni del software.

Soluzione

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

LOW 2.6* X Server Detection

Un server X11 è in ascolto sull'host remoto

Descrizione
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.
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).