Report generated by Nessus™

Metasploitable 2

Giovedì, 1 Giugno 2023 12:06:56 EDT

192.168.50.101

9	4	17	5	69
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Giovedì 1 Giugno 11:36:59 2023

End time: Giovedì 1 Giugno 12:06:56 2023

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilità

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) -

Riepilogo

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

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe 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 JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

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

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Referimenti

CVE	CVE-2020-1745
CVE	CVE-2020-1938

10203 - rexecd Service Detection -

Riepilogo

Il servizio rexecd è in esecuzione sull'host remoto.

Descrizione

Il rexecd è in esecuzione sull'host remoto. Questo servizio è progettato per consentire agli utenti di una rete di eseguire comandi in remoto.

Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi potrebbe essere abusato da un utente malintenzionato per scansionare un host di terze parti.

Soluzione

Commenta la riga exec in /etc/inetd.conf e riavvia il processo inetd.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

51988 - Bind Shell Backdoor Detection -

Riepilogo

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 utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

Soluzione

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

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness -

Riepilogo

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 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 della 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 delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Riferimenti

CVE	CVE-2008-0166

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

Riepilogo

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 organizzare un attacco man in the middle.

Soluzione

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

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2008-0166

11356 - NFS Exported Share Information Disclosure -

Riepilogo

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 utente malintenzionato 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.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

20007 - SSL Version 2 and 3 Protocol Detection -

Riepilogo

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 affette 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 ei client.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supporta nulla di meglio), molti browser web lo implementano 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 entrata in vigore trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" di PCI SSC.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

33850 - Unix Operating System Unsupported Version Detection -

Riepilogo

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

Descrizione

In base al numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto non è 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.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

61708 - VNC Server 'password' Password -

Riepilogo

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 stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password sicura.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

136769 - ISC BIND Service Downgrade / Reflected DoS -

Riepilogo

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 interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione

Aggiornamento alla versione ISC BIND indicata nell'avviso del fornitore.

Risk Factor

Medium

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

References

CVE CVE-2020-8616

42256 - NFS Shares World Readable -

Riepilogo

Il server NFS remoto esporta condivisioni leggibili da tutti.

Descrizione

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (basato su nome host, IP o intervallo IP).

Soluzione

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Riepilogo

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. Nessus considera la forza media come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizzi la suite di crittografia 3DES.

Si noti che è notevolmente più semplice aggirare la crittografia di media potenza se l'attaccante si trova sulla stessa rete fisica.

Soluzione

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

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

CVE CVE-2016-2183

90509 - Samba Badlock Vulnerability -

Riepilogo

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 affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare 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 sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione

Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

Riferimenti

CVE CVE-2016-2118

11213 - HTTP TRACE / TRACK Methods Allowed -

Riepilogo

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.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Riferimenti

CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386

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

Riepilogo

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 server dei nomi remoto 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. Pertanto, è affetto da una vulnerabilità di negazione del servizio (DoS) a causa di un errore di asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando una risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando la chiusura del server.

Si noti che Nessus non ha testato questo problema, ma si è invece basato solo sul numero di versione auto-riportato dell'applicazione.

Soluzione

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Riferimenti

CVE CVE-2020-8622

136808 - ISC BIND Denial of Service -

Riepilogo

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 basato solo sul numero di versione auto-riportato dell'applicazione.

Soluzione

Aggiorna alla versione con patch più strettamente correlata alla tua attuale versione di BIND.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti

CVE CVE-2020-8617

57608 - SMB Signing not required -

Riepilogo

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 del criterio "Server di rete Microsoft: aggiungi firma digitale alle comunicazioni (sempre)". Su Samba, l'impostazione si chiama "firma del server". Vedere i collegamenti "vedi anche" per ulteriori dettagli.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

52611 - SMTP Service STARTTLS Plaintext Command Injection -

Riepilogo

Il servizio di posta remota consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

Descrizione

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase del protocollo di testo in chiaro che verranno eseguiti durante la fase del protocollo di testo cifrato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

Soluzione

Contattare il fornitore per vedere se è disponibile un aggiornamento.

Risk Factor

Medium

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

Riferimenti

CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165

90317 - SSH Weak Algorithms Supported -

Riepilogo

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 la cifratura a flusso Arcfour o nessuna cifratura. 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.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

31705 - SSL Anonymous Cipher Suites Supported -

Riepilogo

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 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

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

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

CVE	CVE-2007-1858

51192 - SSL Certificate Cannot Be Trusted-

Riepilogo

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:

- 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 certificato autofirmato non riconosciuto 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-the-middle contro l'host remoto.

Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

Risk Factor

Medium
CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

15901 - SSL Certificate Expiry -

Riepilogo

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 sono già scaduti.

Soluzione

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

Risk Factor

Medium
CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

45411 - SSL Certificate with Wrong Hostname -

Riepilogo

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.

Risk Factor

Medium
CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

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

Riepilogo

L'host remoto potrebbe essere interessato da una vulnerabilità che consente a un utente malintenzionato remoto di decrittografare potenzialmente il traffico TLS acquisito.

Descrizione

L'host remoto supporta SSLv2 e pertanto può essere interessato da una vulnerabilità che consente un attacco Oracle di riempimento Bleichenbacher cross-protocol 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.

Soluzione

Disabilita SSLv2 ed esporta 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.

Risk Factor

Medium
CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

CVE CVE-2016-0800

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Riepilogo

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 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.

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.

Risk Factor

Medium
CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Riferimenti

CVE CVE-2013-2566

CVE CVE-2015-2808

57582 - SSL Self-Signed Certificate -

Riepilogo

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 l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL poiché chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto.

Si noti che questo plug-in non controlla le catene di certificati che terminano con un certificato non autofirmato, ma firmato da un'autorità di certificazione non riconosciuta.

Soluzione

Acquista o genera un certificato SSL appropriato per questo servizio.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

26928 - SSL Weak Cipher Suites Supported -

Riepilogo

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.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

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

Riepilogo

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 utente malintenzionato 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 esempio 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.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

Riferimenti

CVE CVE-2015-0204

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

Riepilogo

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 POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati 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 a 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 possono 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.

Soluzione

Disabilita SSLv3.

I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS finché SSLv3 non può essere disabilitato.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

Riferimenti

CVE CVE-2014-3566

104743 - TLS Version 1.0 Protocol Detection -

Riepilogo

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 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero essere utilizzate 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 dei punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non soggetti a exploit noti.

Soluzione

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

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

70658 - SSH Server CBC Mode Ciphers Enabled -

Riepilogo

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 di recuperare il messaggio in chiaro dal testo cifrato.

Si noti che questo plug-in controlla solo le opzioni del server SSH e non controlla le versioni software vulnerabili.

Soluzione

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

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Riferimenti

CVE	CVE-2008-5161

153953 - SSH Weak Key Exchange Algorithms Enabled -

Riepilogo

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 di chiavi che NON DOVREBBERO e NON DEVONO essere abilitati.

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 verifica solo le opzioni del server SSH e non controlla le versioni software vulnerabili.

Soluzione

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

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

71049 - SSH Weak MAC Algorithms Enabled -

Riepilogo

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 considerati deboli.

Si noti che questo plug-in verifica solo le opzioni del server SSH e non controlla le versioni software vulnerabili.

Soluzione

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

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

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

Riepilogo

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 la 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.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

Riferimenti

CVE CVE-2015-4000

10407 - X Server Detection -

Riepilogo

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 funzionalità client/server X11 non viene utilizzata, disabilitare completamente il supporto TCP in X11 (-nolisten tcp).

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

21186 - AJP Connector Detection -

Riepilogo

C'è un connettore AJP in ascolto sull'host remoto.

Descrizione

L'host remoto esegue un connettore AJP (Apache JServ Protocol), un servizio mediante il quale un server Web autonomo come Apache comunica su TCP con un contenitore servlet Java come Tomcat.

Soluzione

n/a

Risk Factor

None

18261 - Apache Banner Linux Distribution Disclosure -

Riepilogo

Il nome della distribuzione Linux in esecuzione sull'host remoto è stato trovato nel banner del server web.

Descrizione

Nessus è stato in grado di estrarre il banner del server Web Apache e determinare quale distribuzione Linux è in esecuzione sull'host remoto.

Soluzione

Se non desideri visualizzare queste informazioni, modifica "httpd.conf" e imposta la direttiva "ServerTokens Prod" e riavvia Apache.

Risk Factor

None

48204 - Apache HTTP Server Version -

Riepilogo

È possibile ottenere il numero di versione del server HTTP Apache remoto.

Descrizione

L'host remoto esegue Apache HTTP Server, un server Web open source. Era possibile leggere il numero di versione dal banner.

Soluzione

Soluzione

n/a

Risk Factor

None

84574 - Backported Security Patch Detection (PHP) -

Riepilogo

Le patch di sicurezza sono state trasferite.

Descrizione

Le patch di sicurezza potrebbero essere state 'portate indietro' all'installazione remota di PHP senza modificarne il numero di versione.

I controlli basati su banner sono stati disabilitati per evitare falsi positivi.

Si noti che questo test è solo informativo e non denota alcun problema di sicurezza.

Soluzione

n/a

Risk Factor

None

39520 - Backported Security Patch Detection (SSH) -

Riepilogo

Le patch di sicurezza sono sottoposte a backport.

Descrizione

Le patch di sicurezza potrebbero essere state trasferite al server SSH remoto senza modificarne il numero di versione.

I controlli basati su banner sono stati disabilitati per evitare falsi positivi.

Si noti che questo test è solo informativo e non denota alcun problema di sicurezza.

Soluzione

n/a

Risk Factor

None

39521 - Backported Security Patch Detection (WWW)-

Riepilogo

Le patch di sicurezza sono sottoposte a backport.

Descrizione

Le patch di sicurezza potrebbero essere state trasferite al server HTTP remoto senza modificarne il numero di versione.

I controlli basati su banner sono stati disabilitati per evitare falsi positivi.

Si noti che questo test è solo informativo e non denota alcun problema di sicurezza.

Soluzione

n/a

Risk Factor

None

45590 - Common Platform Enumeration (CPE) -

Riepilogo

E’ stato possibile enumerare i nomi CPE che corrispondevano sul sistema remoto.

Descrizione

Utilizzando le informazioni ottenute da una scansione Nessus, questo plug-in segnala le corrispondenze CPE (Common Platform Enumeration) per vari prodotti hardware e software trovati su un host.

Si noti che se un CPE ufficiale non è disponibile per il prodotto, questo plug-in calcola il miglior CPE possibile in base alle informazioni disponibili dalla scansione.

Soluzione

n/a

Risk Factor

None

10028 - DNS Server BIND version Directive Remote Version Detection -

Riepilogo

È possibile ottenere il numero di versione del server DNS remoto.

Descrizione

L'host remoto esegue BIND o un altro server DNS che riporta il proprio numero di versione quando riceve una richiesta speciale per il testo "version.bind" nel dominio "chaos".

Questa versione non è necessariamente accurata e potrebbe anche essere falsificata, poiché alcuni server DNS inviano le informazioni sulla base di un file di configurazione.

Soluzione

È possibile nascondere il numero di versione di BIND utilizzando la direttiva 'version' nella sezione 'options' in named.conf.

Risk Factor

None

11002 - DNS Server Detection -

Riepilogo

Un server DNS è in ascolto sull'host remoto.

Descrizione

Il servizio remoto è un server DNS (Domain Name System), che fornisce una mappatura tra nomi host e indirizzi IP.

Soluzione

Disabilita questo servizio se non è necessario o limita l'accesso agli host interni solo se il servizio è disponibile esternamente.

Risk Factor

None

72779 - DNS Server Version Detection -

Riepilogo

Nessus è stato in grado di ottenere informazioni sulla versione sul server DNS remoto.

Descrizione

Nessus è stato in grado di ottenere informazioni sulla versione inviando una speciale query di record TXT all'host remoto.

Si noti che questa versione non è necessariamente accurata e potrebbe anche essere falsificata, poiché alcuni server DNS inviano le informazioni sulla base di un file di configurazione.

Soluzione

n/a

Risk Factor

None

35371 - DNS Server hostname.bind Map Hostname Disclosure -

Riepilogo

Il server DNS rivela il nome dell'host remoto.

Descrizione

È possibile conoscere il nome host remoto interrogando il server DNS remoto per "hostname.bind" nel dominio CHAOS.

Soluzione

Potrebbe essere possibile disabilitare questa funzione. Consultare la documentazione del fornitore per ulteriori informazioni.

Risk Factor

None

132634 - Deprecated SSLv2 Connection Attempts -

Riepilogo

Nell'ambito della scansione sono state tentate connessioni sicure che utilizzano un protocollo obsoleto

Descrizione

Questo plug-in enumera e segnala tutte le connessioni SSLv2 che sono state tentate come parte di una scansione. Questo protocollo è stato ritenuto proibito dal 2011 a causa di vulnerabilità di sicurezza e la maggior parte delle principali librerie ssl come openssl, nss, mbed e wolfssl non forniscono questa funzionalità nelle loro versioni più recenti. Questo protocollo è stato deprecato in Nessus 8.9 e versioni successive.

Soluzione

N/A

Risk Factor

None

54615 - Device Type -

Riepilogo

È possibile indovinare il tipo di dispositivo remoto.

Descrizione

In base al sistema operativo remoto, è possibile determinare qual è il tipo di sistema remoto (ad esempio: una stampante, un router, un computer generico, ecc.).

Soluzione

n/a

Risk Factor

None

10092 - FTP Server Detection -

Riepilogo

Un server FTP è in ascolto su una porta remota.

Descrizione

E' possibile ottenere il banner del server FTP remoto collegandosi ad una porta remota.

Soluzione

n/a

Risk Factor

None

10107 - HTTP Server Type and Version -

Riepilogo

Un server Web è in esecuzione sull'host remoto.

Descrizione

Questo plug-in tenta di determinare il tipo e la versione del server Web remoto.

Soluzione

n/a

Risk Factor

None

24260 - HyperText Transfer Protocol (HTTP) Information -

Riepilogo

È possibile estrarre alcune informazioni sulla configurazione HTTP remota.

Descrizione

Questo test fornisce alcune informazioni sul protocollo HTTP remoto: la versione utilizzata, se HTTP Keep-Alive e il pipelining HTTP sono abilitati, ecc...

Questo test è solo informativo e non denota alcun problema di sicurezza.

Soluzione

n/a

Risk Factor

None

10114 - ICMP Timestamp Request Remote Date Disclosure -

Riepilogo

È possibile determinare l'ora esatta impostata sull'host remoto.

Descrizione

L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina mirata, che può aiutare un utente malintenzionato remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.

I timestamp restituiti dai computer che eseguono Windows Vista/7/2008/2008 R2 sono deliberatamente errati, ma di solito entro 1000 secondi dall'ora effettiva del sistema.

Soluzione

Filtrare le richieste timestamp ICMP (13) e le risposte timestamp ICMP in uscita (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

Riferimenti

CVE CVE-1999-0524

11156 - IRC Daemon Version Detection -

Riepilogo

L'host remoto è un server IRC.

Descrizione

Questo plugin determina la versione del demone IRC.

Soluzione

n/a

Risk Factor

None

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure -

Riepilogo

È possibile ottenere informazioni sulla rete.

Descrizione

È stato possibile ottenere l'elenco di navigazione del sistema Windows remoto inviando una richiesta alla pipe LANMAN. L'elenco di ricerca è l'elenco dei sistemi Windows più vicini dell'host remoto.

Soluzione

n/a

Risk Factor

None

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Riepilogo

È stato possibile ottenere informazioni sul sistema operativo remoto.

Descrizione

Nessus è stato in grado di ottenere il nome e la versione del sistema operativo remoto (Windows e/o Samba) inviando una richiesta di autenticazione alla porta 139 o 445. Si noti che questo plug-in richiede che SMB sia abilitato sull'host.

Soluzione

n/a

Risk Factor

None

11011 - Microsoft Windows SMB Service Detection -

Riepilogo

Un servizio di condivisione file/stampa è in ascolto sull'host remoto.

Descrizione

Il servizio remoto comprende il protocollo CIFS (Common Internet File System) o Server Message Block (SMB), utilizzato per fornire accesso condiviso a file, stampanti, ecc. tra i nodi di una rete.

Soluzione

n/a

Risk Factor

None

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Riepilogo

È stato possibile ottenere informazioni sulla versione di SMB in esecuzione sull'host remoto.

Descrizione

Nessus è stato in grado di ottenere la versione di SMB in esecuzione sull'host remoto inviando una richiesta di autenticazione alla porta 139 o 445.

Si noti che questo plug-in è un controllo remoto e non funziona sugli agenti.

Soluzione

n/a

Risk Factor

None

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Riepilogo

È stato possibile ottenere informazioni sui dialetti di SMB2 e SMB3 disponibili sull'host remoto.

Descrizione

Nessus è stato in grado di ottenere il set di dialetti SMB2 e SMB3 in esecuzione sull'host remoto inviando una richiesta di autenticazione alla porta 139 o 445.

Soluzione

n/a

Risk Factor

None

10437 - NFS Share Export List -

Riepilogo

Il server NFS remoto esporta un elenco di condivisioni.

Descrizione

Questo plugin recupera l'elenco delle condivisioni esportate NFS.

Soluzione

Assicurarsi che ogni condivisione sia destinata all'esportazione.

Risk Factor

None

11219 - Nessus SYN scanner -

Riepilogo

È possibile determinare quali porte TCP sono aperte.

Descrizione

Questo plugin è un port scanner SYN 'semiaperto'. Sarà ragionevolmente veloce anche contro un obiettivo protetto da firewall.

Si noti che le scansioni SYN sono meno intrusive delle scansioni TCP (connessione completa) contro servizi interrotti, ma potrebbero causare problemi per firewall meno robusti e anche lasciare connessioni non chiuse sulla destinazione remota, se la rete è carica.

Soluzione

Proteggi il tuo obiettivo con un filtro IP.

Risk Factor

None

19506 - Nessus Scan Information -

Riepilogo

Questo plugin visualizza informazioni sulla scansione di Nessus.

Descrizione

Questo plugin visualizza, per ogni host testato, informazioni sulla scansione stessa:

- La versione del set di plugin.
- Il tipo di scanner (Nessus o Nessus Home).
- La versione del Nessus Engine.
- Il/i port scanner utilizzato/i.
- L'intervallo di porte scansionato.
- Il tempo di andata e ritorno del ping
- Se sono possibili controlli di gestione delle patch con credenziali o di terze parti.
- Se è abilitata la visualizzazione delle patch sostituite
- La data della scansione.
- La durata della scansione.
- Il numero di host analizzati in parallelo.
- Il numero di controlli eseguiti in parallelo.

Soluzione

n/a

Risk Factor

None

11936 - OS Identification -

Riepilogo

È possibile indovinare il sistema operativo remoto.

Descrizione

Utilizzando una combinazione di sonde remote (ad esempio, TCP/IP, SMB, HTTP, NTP, SNMP, ecc.), è possibile indovinare il nome del sistema operativo remoto in uso. A volte è anche possibile indovinare la versione del sistema operativo.

Soluzione

n/a

Risk Factor

None

117886 - OS Security Patch Assessment Not Available -

Riepilogo

OS Security Patch Assessment non è disponibile.

Descrizione

OS Security Patch Assessment non è disponibile sull'host remoto.

Ciò non indica necessariamente un problema con la scansione.

Le credenziali potrebbero non essere state fornite, la valutazione della patch di sicurezza del sistema operativo potrebbe non essere supportata per la destinazione, la destinazione potrebbe non essere stata identificata o potrebbe essersi verificato un altro problema che ha impedito la disponibilità della valutazione della patch di sicurezza del sistema operativo. Vedi l'output del plugin per i dettagli.

Questo plug-in segnala le informazioni di non errore che incidono sulla disponibilità della valutazione delle patch di sicurezza del sistema operativo. Le informazioni sull'errore vengono riportate dal plug-in 21745: "OS Security Patch Assessment failed". Se un host di destinazione non è supportato per OS Security Patch Assessment, il plug-in 110695: 'OS Security Patch Assessment Checks Not Supported' segnalerà contemporaneamente a questo plug-in.

Soluzione

n/a

Risk Factor

None

50845 - OpenSSL Detection -

Riepilogo

Il servizio remoto sembra utilizzare OpenSSL per crittografare il traffico.

Descrizione

Sulla base della sua risposta a una richiesta TLS con un'estensione del nome del server appositamente predisposta, sembra che il servizio remoto stia utilizzando la libreria OpenSSL per crittografare il traffico.

Tieni presente che questo plug-in può rilevare solo le implementazioni OpenSSL che hanno abilitato il supporto per le estensioni TLS (RFC 4366).

Soluzione

n/a

Risk Factor

None

48243 - PHP Version Detection -

Riepilogo

È stato possibile ottenere il numero di versione dell'installazione remota di PHP.

Descrizione

Nessus è stato in grado di determinare la versione di PHP disponibile sul server web remoto.

Soluzione

n/a

Risk Factor

None

66334 - Patch Report -

Riepilogo

Nell'host remoto mancano diverse patch.

Descrizione

Nell'host remoto mancano una o più patch di sicurezza. Questo plugin elenca la versione più recente di ciascuna patch da installare per assicurarsi che l'host remoto sia aggiornato.

Nota: poiché l'impostazione "Mostra le patch mancanti che sono state sostituite" nel criterio di scansione dipende da questo plug-in, verrà sempre eseguito e non può essere disattivato.

Soluzione

Installa le patch elencate di seguito.

Risk Factor

None

118224 - PostgreSQL STARTTLS Support -

Riepilogo

Il servizio remoto supporta la crittografia del traffico.

Descrizione

Il server PostgreSQL remoto supporta l'uso della crittografia avviata durante il pre-accesso per passare da un canale di comunicazione in chiaro a un canale di comunicazione crittografato.

Soluzione

n/a

Risk Factor

None

26024 - PostgreSQL Server Detection -

Riepilogo

Un servizio di database è in ascolto sull'host remoto.

Descrizione

Il servizio remoto è un server di database PostgreSQL o un derivato come EnterpriseDB.

Soluzione

Se lo desideri, limita il traffico in entrata a questa porta.

Risk Factor

None

22227 - RMI Registry Detection -

Riepilogo

Un registro RMI è in ascolto sull'host remoto.

Descrizione

L'host remoto esegue un registro RMI, che funge da servizio di denominazione bootstrap per la registrazione e il recupero di oggetti remoti con nomi semplici nel sistema Java Remote Method Invocation (RMI).

Soluzione

n/a

Risk Factor

None

11111 - RPC Services Enumeration -

Riepilogo

Un servizio ONC RPC è in esecuzione sull'host remoto.

Descrizione

Inviando una richiesta DUMP al portmapper, è stato possibile enumerare i servizi ONC RPC in esecuzione sulla porta remota. Utilizzando queste informazioni, è possibile connettersi e collegarsi a ciascun servizio inviando una richiesta RPC alla porta remota.

Soluzione

n/a

Risk Factor

None

53335 - RPC portmapper (TCP) -

Riepilogo

Un portmapper ONC RPC è in esecuzione sull'host remoto.

Descrizione

Il portmapper RPC è in esecuzione su questa porta.

Il portmapper consente a qualcuno di ottenere il numero di porta di ciascun servizio RPC in esecuzione sull'host remoto inviando più richieste di ricerca o una richiesta DUMP.

Soluzione

n/a

Risk Factor

None

10223 - RPC portmapper Service Detection -

Riepilogo

Un portmapper ONC RPC è in esecuzione sull'host remoto.

Descrizione

Il portmapper RPC è in esecuzione su questa porta.

Il portmapper consente a qualcuno di ottenere il numero di porta di ciascun servizio RPC in esecuzione sull'host remoto inviando più richieste di ricerca o una richiesta DUMP.

Soluzione

n/a

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

Riferimenti

CVE	CVE-1999-0632

10263 - SMTP Server Detection -

Riepilogo

Un server SMTP è in ascolto sulla porta remota.

Descrizione

L'host remoto esegue un server di posta (SMTP) su questa porta.

Poiché i server SMTP sono il bersaglio degli spammer, si consiglia di disabilitarlo se non lo si utilizza.

Soluzione

Disabilita questo servizio se non lo usi o filtra il traffico in entrata verso questa porta.

Risk Factor

None

42088 - SMTP Service STARTTLS Command Support -

Riepilogo

Il servizio di posta remota supporta la crittografia del traffico.

Descrizione

Il servizio SMTP remoto supporta l'uso del comando 'STARTTLS' per passare da un canale di comunicazione in chiaro a un canale di comunicazione crittografato.

Soluzione

n/a

Risk Factor

None

70657 - SSH Algorithms and Languages Supported -

Riepilogo

Un server SSH è in ascolto su questa porta.

Descrizione

Questo script rileva quali algoritmi e linguaggi sono supportati dal servizio remoto per la crittografia delle comunicazioni.

Soluzione

n/a

Risk Factor

None

149334 - SSH Password Authentication Accepted -

Riepilogo

Il server SSH sull'host remoto accetta l'autenticazione della password.

Descrizione

Il server SSH sull'host remoto accetta l'autenticazione della password.

Soluzione

n/a

Risk Factor

None

10881 - SSH Protocol Versions Supported -

Riepilogo

Un server SSH è in esecuzione sull'host remoto.

Descrizione

Questo plugin determina le versioni del protocollo SSH supportate dal daemon SSH remoto.

Soluzione

n/a

Risk Factor

None

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Riepilogo

Il server SSH remoto è configurato per abilitare gli algoritmi HMAC SHA-1.

Descrizione

Il server SSH remoto è configurato per abilitare gli algoritmi HMAC SHA-1.

Sebbene il NIST abbia formalmente deprecato l'uso di SHA-1 per le firme digitali, SHA-1 è ancora considerato sicuro per HMAC poiché la sicurezza di HMAC non si basa sulla resistenza alla collisione della funzione hash sottostante.

Si noti che questo plug-in controlla solo le opzioni del server SSH remoto.

Soluzione

n/a

Risk Factor

None

10267 - SSH Server Type and Version Information -

Riepilogo

Un server SSH è in ascolto su questa porta.

Descrizione

È possibile ottenere informazioni sul server SSH remoto inviando una richiesta di autenticazione vuota.

Soluzione

n/a

Risk Factor

None

56984 - SSL / TLS Versions Supported -

Riepilogo

Il servizio remoto crittografa le comunicazioni.

Descrizione

Questo plug-in rileva quali versioni SSL e TLS sono supportate dal servizio remoto per la crittografia delle comunicazioni.

Soluzione

n/a

Risk Factor

None

45410 - SSL Certificate 'commonName' Mismatch -

Riepilogo

L'attributo 'commonName' (CN) nel certificato SSL non corrisponde al nome host.

Descrizione

Il servizio in esecuzione sull'host remoto presenta un certificato SSL per il quale l'attributo 'commonName' (CN) non corrisponde al nome host su cui il servizio è in ascolto.

Soluzione

Se la macchina ha più nomi, assicurarsi che gli utenti si connettano al servizio tramite il nome host DNS che corrisponde al nome comune nel certificato.

Risk Factor

None

10863 - SSL Certificate Information -

Riepilogo

Questo plugin visualizza il certificato SSL.

Descrizione

Questo plug-in si connette a tutte le porte relative a SSL e tenta di estrarre e scaricare il certificato X.509.

Soluzione

n/a

Risk Factor

None

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Riepilogo

Il servizio remoto supporta l'uso di crittografie SSL Cipher Block Chaining, che combinano i blocchi precedenti con quelli successivi.

Descrizione

L'host remoto supporta l'utilizzo di crittografie SSL che operano in modalità Cipher Block Chaining (CBC). Queste suite di crittografia offrono una sicurezza aggiuntiva rispetto alla modalità Electronic Codebook (ECB), ma possono potenzialmente far trapelare informazioni se utilizzate in modo improprio.

Soluzione

n/a

Risk Factor

None

21643 - SSL Cipher Suites Supported -

Riepilogo

Il servizio remoto crittografa le comunicazioni utilizzando SSL.

Descrizione

Questo plug-in rileva quali cifrari SSL sono supportati dal servizio remoto per la crittografia delle comunicazioni.

Soluzione

n/a

Risk Factor

None

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Riepilogo

Il servizio remoto supporta l'uso di cifrari SSL Perfect Forward Secrecy, che mantengono la riservatezza anche in caso di furto della chiave.

Descrizione

L'host remoto supporta l'uso di crittografie SSL che offrono la crittografia Perfect Forward Secrecy (PFS). Queste suite di cifratura assicurano che il traffico SSL registrato non possa essere interrotto in una data futura se la chiave privata del server viene compromessa.

Soluzione

n/a

Risk Factor

None

51891 - SSL Session Resume Supported -

Riepilogo

L'host remoto consente di riprendere le sessioni SSL.

Descrizione

Questo script rileva se un host consente di riprendere le sessioni SSL eseguendo un handshake SSL completo per ricevere un ID di sessione e quindi riconnettersi con l'ID di sessione utilizzato in precedenza. Se il server accetta l'ID di sessione nella seconda connessione, il server mantiene una cache di sessioni che possono essere riprese.

Soluzione

n/a

Risk Factor

None

156899 - SSL/TLS Recommended Cipher Suites -

Riepilogo

L'host remoto annuncia crittografie SSL/TLS sconsigliate.

Descrizione

L'host remoto ha porte SSL/TLS aperte che pubblicizzano suite di cifratura sconsigliate. Si consiglia di abilitare il supporto solo per le seguenti suite di cifratura:

TLSv1.3:

- 0x13,0x01TLS_AES_128_GCM_SHA256

- 0x13,0x02TLS_AES_256_GCM_SHA384

- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

Questa è la configurazione consigliata per la stragrande maggioranza dei servizi, poiché è altamente sicura e compatibile con quasi tutti i client rilasciati negli ultimi cinque (o più) anni.

Soluzione

Abilita solo il supporto per le suite di crittografia consigliate.

Risk Factor

None

25240 - Samba Server Detection -

Riepilogo

Un server SMB è in esecuzione sull'host remoto.

Descrizione

L'host remoto esegue Samba, un server CIFS/SMB per Linux e Unix.

Soluzione

n/a

Risk Factor

None

104887 - Samba Version -

Riepilogo

È stato possibile ottenere la versione samba dal sistema operativo remoto.

Descrizione

Nessus è stato in grado di ottenere la versione samba dall'operatore remoto inviando una richiesta di autenticazione alla porta 139 o 445. Si noti che questo plug-in richiede che SMB1 sia abilitato sull'host.

Soluzione

n/a

Risk Factor

None

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Riepilogo

L'host Windows remoto supporta il protocollo SMBv1.

Descrizione

L'host Windows remoto supporta Server Message Block Protocol versione 1 (SMBv1). Microsoft consiglia agli utenti di interrompere l'utilizzo di SMBv1 a causa della mancanza di funzionalità di sicurezza incluse nelle versioni successive di SMB. Inoltre, secondo quanto riferito, il gruppo Shadow Brokers ha un exploit che colpisce SMB; tuttavia, non è noto se l'exploit riguardi SMBv1 o un'altra versione. In risposta a ciò, US-CERT consiglia agli utenti di disabilitare le best practice SMBv1 per SMB per mitigare questi potenziali problemi.

Soluzione

Disabilita SMBv1 in base alle istruzioni del fornitore in Microsoft KB2696547. Inoltre, blocca SMB direttamente bloccando la porta TCP 445 su tutti i dispositivi di confine della rete. Per SMB sull'API NetBIOS, bloccare le porte TCP 137/139 e le porte UDP 137/138 su tutti i dispositivi di confine della rete.

Risk Factor

None

22964 - Service Detection -

Riepilogo

Il servizio remoto potrebbe essere identificato.

Descrizione

Nessus è stato in grado di identificare il servizio remoto tramite il suo banner o guardando il messaggio di errore che invia quando riceve una richiesta HTTP.

Soluzione

n/a

Risk Factor

None

17975 - Service Detection (GET request) -

Riepilogo

Il servizio remoto potrebbe essere identificato.

Descrizione

È stato possibile identificare il servizio remoto tramite il suo banner o guardando il messaggio di errore che invia quando riceve una richiesta HTTP.

Soluzione

n/a

Risk Factor

None

25220 - TCP/IP Timestamps Supported -

Riepilogo

Il servizio remoto implementa i timestamp TCP.

Descrizione

L'host remoto implementa i timestamp TCP, come definito da RFC1323. Un effetto collaterale di questa funzione è che a volte è possibile calcolare il tempo di attività dell'host remoto.

Soluzione

n/a

Risk Factor

None

11819 - TFTP Daemon Detection -

Riepilogo

Un server TFTP è in ascolto sulla porta remota.

Descrizione

L'host remoto esegue un demone TFTP (Trivial File Transfer Protocol). TFTP viene spesso utilizzato da router e host senza disco per recuperare la propria configurazione. Può anche essere utilizzato dai worm per propagarsi.

Soluzione

Disabilita questo servizio se non lo usi.

Risk Factor

None

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Riepilogo

Nessus è stato in grado di trovare porte comuni utilizzate per i controlli locali, tuttavia, non sono state fornite credenziali nella politica di scansione.

Descrizione

Nessus non è stato in grado di eseguire correttamente l'autenticazione direttamente alla destinazione remota su un protocollo di autenticazione disponibile. Nessus è stato in grado di connettersi alla porta remota e identificare che il servizio in esecuzione sulla porta supporta un protocollo di autenticazione, ma Nessus non è riuscito ad autenticarsi al servizio remoto utilizzando le credenziali fornite. Potrebbe essersi verificato un errore del protocollo che ha impedito il tentativo di autenticazione oppure tutte le credenziali fornite per il protocollo di autenticazione potrebbero non essere valide. Vedere l'output del plug-in per i dettagli sull'errore.

Si prega di notare quanto segue:

- Questo plug-in segnala per protocollo, quindi è possibile fornire credenziali valide per un protocollo e non per un altro. Ad esempio, l'autenticazione può riuscire tramite SSH ma fallire tramite SMB, mentre non sono state fornite credenziali per un servizio SNMP disponibile.

- Fornire credenziali valide per tutti i protocolli di autenticazione disponibili può migliorare la copertura della scansione, ma il valore dell'autenticazione riuscita per un determinato protocollo può variare da destinazione a destinazione a seconda di quali dati (se presenti) vengono raccolti dalla destinazione tramite quel protocollo. Ad esempio, l'autenticazione riuscita tramite SSH è più preziosa per le destinazioni Linux che per le destinazioni Windows e allo stesso modo l'autenticazione riuscita tramite SMB è più preziosa per le destinazioni Windows che per le destinazioni Linux.

Soluzione

n/a

Risk Factor

None

10287 - Traceroute Information -

Riepilogo

È stato possibile ottenere informazioni sul traceroute.

Descrizione

Crea un traceroute verso l'host remoto.

Soluzione

n/a

Risk Factor

None

11154 - Unknown Service Detection: Banner Retrieval -

Riepilogo

C'è un servizio sconosciuto in esecuzione sull'host remoto.

Descrizione

Nessus non è stato in grado di identificare un servizio sull'host remoto anche se ha restituito un banner di qualche tipo.

Soluzione

n/a

Risk Factor

None

19288 - VNC Server Security Type Detection -

Riepilogo

Un server VNC è in esecuzione sull'host remoto.

Descrizione

Questo script controlla la versione del protocollo del server VNC remoto ei "tipi di sicurezza" disponibili.

Soluzione

n/a

Risk Factor

None

65792 - VNC Server Unencrypted Communication Detection -

Riepilogo

Un server VNC con uno o più "tipi di sicurezza" non crittografati è in esecuzione sull'host remoto.

Descrizione

Questo script controlla la versione del protocollo del server VNC remoto e i "tipi di sicurezza" disponibili per determinare se sono in uso o disponibili "tipi di sicurezza" non crittografati.

Soluzione

n/a

Risk Factor

None

10342 - VNC Software Detection -

Riepilogo

L'host remoto esegue un software di visualizzazione remota (VNC).

Descrizione

L'host remoto esegue VNC (Virtual Network Computing), che utilizza il protocollo RFB (Remote Framebuffer) per fornire l'accesso remoto alle interfacce utente grafiche e quindi consente di visualizzare una console sull'host remoto su un altro.

Soluzione

Assicurati che l'uso di questo software sia effettuato in conformità con la politica di sicurezza della tua organizzazione e filtra il traffico in entrata verso questa porta.

Risk Factor

None

135860 - WMI Not Available -

Riepilogo

Impossibile eseguire query WMI sull'host remoto.

Descrizione

WMI (Windows Management Instrumentation) non è disponibile sull'host remoto su DCOM. Le query WMI vengono utilizzate per raccogliere informazioni sull'host remoto, come il suo stato corrente, la configurazione dell'interfaccia di rete, ecc.

Senza queste informazioni, Nessus potrebbe non essere in grado di identificare il software installato o le vulnerabilità di sicurezza esistenti sull'host remoto.

Soluzione

n/a

Risk Factor

None

11424 - WebDAV Detection -

Riepilogo

Il server remoto è in esecuzione con WebDAV abilitato.

Descrizione

WebDAV è un'estensione standard del settore della specifica HTTP.

Aggiunge una capacità per gli utenti autorizzati di aggiungere e gestire in remoto il contenuto di un server web.

Se non utilizzi questa estensione, dovresti disabilitarla.

Soluzione

n/a

Risk Factor

None

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure -

Riepilogo

È stato possibile ottenere il nome di rete dell'host remoto

Descrizione

L'host remoto è in ascolto sulla porta UDP 137 o sulla porta TCP 445 e risponde alle richieste NetBIOS nbtscan o SMB.

Si noti che questo plug-in raccoglie informazioni da utilizzare in altri plug-in, ma non genera esso stesso un report.

Soluzione

n/a

Risk Factor

None

52703 - vsftpd Detection -

Riepilogo

Un server FTP è in ascolto sulla porta remota.

Descrizione

L'host remoto esegue vsftpd, un server FTP per sistemi simili a UNIX scritto in C.

Soluzione

n/a

Risk Factor

None