



# Metasploitable\_scan\_1

---

Rapporto generato da Nessus™

Gio, 01 giu 2023 08:05:15 EDT

---

---

SOMMARIO

---

**Vulnerabilità per host**

- 192.168.50.101.....4

---

## **Vulnerabilità per host**

---

192.168.50.101

10

CRITICA

5

ALTO

24

MEDIO

5

BASSO

128

INFORMAZIONE

#### Informazioni sulla scansione

Ora di inizio: gio giu 1 07:25:34 2023 gio

Tempo scaduto: giu giu 1 08:05:15 2023

#### Informazioni sull'ospite

Nome Netbios: Metasploitable

IP: 192.168.50.101

Indirizzo MAC: 08:00:27:0F:70:B4

Sistema operativo: Linux Kernel 2.6 su Ubuntu 8.04 (resistente)

## Vulnerabilità

**134862 - Iniezione richiesta connettore Apache Tomcat A JP (Ghostcat)**

### Sinossi

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. 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 JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

#### Guarda anche

<http://www.nessus.org/u?8ebe6246> <http://www.nessus.org/u?4e287adb> <http://www.nessus.org/u?cbc3d54e> <https://access.redhat.com/security/cve/CVE-2020-1745> <https://access.redhat.com/solutions/4851251> <http://www.nessus.org/u?dd218234>

<http://www.nessus.org/u?dd772531>

<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eafc70>

#### 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.

#### Fattore di rischio

#### Alto

##### Punteggio base CVSS v3.0

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

##### Punteggio temporale CVSS v3.0

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

##### Punteggio base CVSS v2.0

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

##### Punteggio temporale CVSS v2.0

6.5 (CVSS2#E:H/RL:OF/RC:C)

#### Riferimenti

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XRIF	CISA-KNOWN-EXPLOITED:2022/03/17
XRIF	CEA-ID:CEA-2020-0021

#### Informazioni sul plug-in

Pubblicato: 24/03/2020, Modificato: 24/05/2023

#### Uscita del plug-in

tcp/8009/ajp13

Nessus è stato in grado di sfruttare il problema utilizzando la seguente richiesta:

0x0000:	02 02 00 08 48 54 50 2F 31 2E 31 00 00 0F 2F 61 73 64 66 2F	... HTTP/1.1.../asdf/
0x0010:	78 78 78 78 78 2E 6A 73 70 00 00 09 6C 6F 63 61 6C 68 6F 7 3 74	xxxxx.jsp..
0x0020:	00 FF FF 00 09 6C 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0	. localhost.....l
0x0030:	06 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 63 63 65 70	ocalhost..P.....
0x0040:	74 2D 4C 61 6E 67 75 61 67 65 00 00 0E 65 6E 2D 55 53 2C 65 6E	. . mantenere in vita...A
0x0050:	3B 71 3D 30 2E 35 00 A0 08 00 01 30 00 00 0F 41 63 63 65 70 74	ccept-Lingua..
0x0060:	2D 45 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 64 65 66	. en-US,en;q=0.5.
0x0070:	6C 61 74 65 2C 20 73 64 63 68 00 00 0D 43 61 63 68 65 2D 43 6F	. . . 0...Accept-E
0x0080:	6E 74 72 6F 6C 00 00 09 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00	ncoding...gzip,
0x0090:	07 4D 6F 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D 49 6E	sgonfiare, sdch...
0x00A0:	73 65 63 75 72 65 2D 52 65 71 75 65 73 74 73 00 00 01 31 00 A0	Controllo cache...
0x00B0:	01 00 09 74 65 78 74 2F 68 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61	max-età=0.....Lu
0x00C0:	6C 68 6F 73 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C 65	zilla...Aggiorna-
0x00D0:	74 2E 69 6E 63 6C 75 64 65 2E 72 65 7175 65 73 74 5F 75 72 69 00	Richiesta insicura
0x00E0:	00 01 31 00 0A 00 1F 6A 61 76 61 78 2E 73 65 72 76 6C 65 74 2E	s...1.....testo/h
0x00F0:	69 6E 63 6C 75 64 65 2E 70 61 7 4 68 5F 69 6E 66 6F 00 00 10 2F	tml.....localhos
0x0100:	57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C 00 0A 00 22 6A 61	t...javax.servl
0x0110:	76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C 75 64 6 5 2E 73	et.include.reque
0x0120:	65 72 76 6C 65 74 5F 70 61 74 68 00 00 00 00 FF	st_uri...1....ja
0x0130:		vax.servlet.incl
0x0140:		ude.path_info...
0x0150:		/WEB-INF/web.xml
0x0160:		. . . "javax.servle
0x0170:		t.include.servle
0x0180:		t_percorso.....

Ciò ha prodotto il seguente output troncato (limite [...])

## 51988 - Rilevamento Backdoor Bind Shell

### Sinossi

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.

### Fattore di rischio

### Critico

### Punteggio base CVSS v3.0

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

### Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

### Informazioni sul plug-in

Pubblicato: 15/02/2011, Modificato: 11/04/2022

### Uscita del plug-in

tcp/1524/wild\_shell

Nessus è stato in grado di eseguire il comando "id" utilizzando la seguente richiesta:

Ciò ha prodotto il seguente output troncato (limitato a 10 righe):

```
----- taglio ----- root@metasploitable :/#  
uid=0(root) gid=0(root) groups=0(root) root@metasploitable :/#
```

```
----- taglio -----
```

### Sinossi

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.

### Guarda anche

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### 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.

### Fattore di rischio

### Critico

### Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

### Punteggio temporale CVSS v2.0

8.3 (CVSS2#E:F/RL:OF/RC:C)

### Riferimenti

OFFERTA	29179
CVE	CVE-2008-0166
XRIF	CWE: 310

### Sfruttabile con

Core Impact (vero)



Informazioni sul plug-in

---

Pubblicato: 14/05/2008, Modificato: 15/11/2018

Uscita del plug-in

---

tcp/22/ssh

### Sinossi

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.

### Guarda anche

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### 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.

### Fattore di rischio

### Critico

### Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

### Punteggio temporale CVSS v2.0

8.3 (CVSS2#E:F/RL:OF/RC:C)

### Riferimenti

OFFERTA	29179
CVE	CVE-2008-0166
XRIF	CWE: 310

### Sfruttabile con

Core Impact (vero)

Informazioni sul plug-in

---

Pubblicato: 15/05/2008, Modificato: 16/11/2020

Uscita del plug-in

---

tcp/25/smtp

### Sinossi

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.

### Guarda anche

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### 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.

### Fattore di rischio

### Critico

### Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

### Punteggio temporale CVSS v2.0

8.3 (CVSS2#E:F/RL:OF/RC:C)

### Riferimenti

OFFERTA	29179
CVE	CVE-2008-0166
XRIF	CWE: 310

### Sfruttabile con

Core Impact (vero)

Informazioni sul plug-in

---

Pubblicato: 15/05/2008, Modificato: 16/11/2020

Uscita del plug-in

---

tcp/5432/postgresql

## Sinossi

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.

## Fattore di rischio

## Critico

## Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

## Riferimenti

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

## Sfruttabile con

Metasploit (vero)

## Informazioni sul plug-in

Pubblicato: 12/03/2003, Modificato: 17/09/2018

## Uscita del plug-in

udp/2049/rpc-nfs

È possibile montare le seguenti condivisioni NFS:

```
+ /
+ Contenuto di / :
- .
- . .
- bidone
- stivale
- cd rom
```

- dev
- eccetera
- casa
- iniz
- initrd.img
- lib
- perso+trovato
- supporti
- mnt
- nohup.out
- optare
- proc
- radice
- sbin
- srv
- sistema
- tmp
- usr
- var
- vmlinuz

### Sinossi

---

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 e i 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.

### Guarda anche

---

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540> <https://>

[www.openssl.org/~bodo/ssl-poodle.pdf](http://www.openssl.org/~bodo/ssl-poodle.pdf) <http://>

[www.nessus.org/u?5d15ba70](http://www.nessus.org/u?5d15ba70)

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

### 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.

### Fattore di rischio

---

### Critico

### Punteggio base CVSS v3.0

---



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

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Informazioni sul plug-in

Pubblicato: 12/10/2005, Modificato: 04/04/2022

Uscita del plug-in

tcp/25/smtp

- SSLv2 è abilitato e il server supporta almeno una crittografia.

Crittografie a bassa resistenza (<= chiave a 64 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
EXP-RC2-CBC-MD5		RSA(512)	RSAA	RC2-CBC(40)	MD5
esportare					
EXP-RC4-MD5		RSA(512)	RSAA	RC4(40)	MD5
esportare					

Cifrature di media potenza (chiave > 64 bit e < 112 bit o 3DES)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
DES-CBC3-MD5		RSAA	RSAA	3DES-CBC(168)	MD5

Cifrature ad alta resistenza (>= chiave a 112 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
RC4-MD5		RSAA	RSAA	RC4(128)	MD5

I campi sopra sono:

{nome cifrato sostenibile}  
{Codice ID cifrato}  
Kex={scambio di chiavi}  
Auth={autenticazione}  
Encrypt={metodo di crittografia simmetrica}  
MAC={codice di autenticazione del messaggio} {flag di esportazione}

- SSLv3 è abilitato e il server supporta almeno una crittografia. Spiegazione: le suite di cifratura TLS 1.0 e SSL 3.0 possono essere utilizzate con SSLv3

Crittografie a bassa resistenza (<= chiave a 64 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
EXP-EDH-RSA-DES-CBC-SHA		DH(512)	RSAA	DES-CBC(40)	
esportare					
EXP-EDH-RSA-DES-CBC-SHA		DH	RSAA	DES-CBC(56)	SHA
[...]					

### Sinossi

---

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 e i 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.

### Guarda anche

---

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540> <https://>

[www.openssl.org/~bodo/ssl-poodle.pdf](http://www.openssl.org/~bodo/ssl-poodle.pdf) <http://>

[www.nessus.org/u?5d15ba70](http://www.nessus.org/u?5d15ba70)

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

### 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.

### Fattore di rischio

---

### Critico

### Punteggio base CVSS v3.0

---

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

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Informazioni sul plug-in

Pubblicato: 12/10/2005, Modificato: 04/04/2022

Uscita del plug-in

tcp/5432/postgresql

- SSLv3 è abilitato e il server supporta almeno una crittografia. Spiegazione: le suite di cifratura TLS 1.0 e SSL 3.0 possono essere utilizzate con SSLv3

Cifrature di media potenza (chiave > 64 bit e < 112 bit o 3DES)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
EDH-RSA-DES-CBC3-SHA		DH	RSAA	3DES-CBC(168)	
SHA1					
DES-CBC3-SHA		RSAA	RSAA	3DES-CBC(168)	
SHA1					

Cifrature ad alta resistenza (>= chiave a 112 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
DHE-RSA-AES128-SHA		DH	RSAA	AES-CBC(128)	
SHA1					
DHE-RSA-AES256-SHA		DH	RSAA	AES-CBC(256)	
SHA1					
AES128-SHA		RSAA	RSAA	AES-CBC(128)	
SHA1					
AES256-SHA		RSAA	RSAA	AES-CBC(256)	
SHA1					
RC4-SHA		RSAA	RSAA	RC4(128)	
SHA1					

I campi sopra sono:

{nome cifrato sostenibile}  
{Codice ID cifrato}  
Kex={scambio di chiavi}  
Auth={autenticazione}  
Encrypt={metodo di crittografia simmetrica}  
MAC={codice di autenticazione del messaggio} {flag di  
esportazione}

## Sinossi

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.

## Fattore di rischio

Critico

## Punteggio base CVSS v3.0

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

## Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

## Riferimenti

XRIF	IAV:0001-A-0502
XRIF	IAVA:0001-A-0648

## Informazioni sul plug-in

Pubblicato: 2008/08/08, Modificato: 2023/05/18

## Uscita del plug-in

TCP/0

Il supporto di Ubuntu 8.04 è terminato il 12-05-2011 (Desktop) / 09-05-2013 (Server). Aggiorna a Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

Per ulteriori informazioni, vedere: <https://wiki.ubuntu.com/Releases>

## 61708 - Password 'password' del server VNC

### Sinossi

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.

### Fattore di rischio

### Critico

### Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

### Informazioni sul plug-in

Pubblicato: 29/08/2012, Modificato: 24/09/2015

### Uscita del plug-in

tcp/5900/vnc

Nessus ha effettuato l'accesso utilizzando una password di "password".

### Sinossi

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.

Guarda anche

<https://kb.isc.org/docs/cve-2020-8616>

### Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Gravità

IO

Riferimenti

CVE	CVE-2020-8616
XRIF	IAVA:2020-A-0217-S

#### Informazioni sul plug-in

---

Pubblicato: 22/05/2020, Modificato: 26/06/2020

#### Uscita del plug-in

---

udp/53/dns

Versione installata: 9.4.2 Versione  
fissa : 9.11.19

## Sinossi

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).

Guarda anche

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

## Soluzione

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 26/10/2009, Modificato: 05/05/2020

Uscita del plug-in

tcp/2049/rpc-nfs

Le seguenti condivisioni non hanno restrizioni di accesso:

/ \*



## Sinossi

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.

## Guarda anche

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>

<https://sweet32.info>

## Soluzione

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

## Fattore di rischio

medio

## Punteggio base CVSS v3.0

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

## Punteggio base CVSS v2.0

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

## Riferimenti

CVE CVE-2016-2183

## Informazioni sul plug-in

Pubblicato: 23/11/2009, Modificato: 03/02/2021

## Uscita del plug-in

tcp/25/smtp

Cifrature di media potenza (chiave > 64 bit e < 112 bit o 3DES)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	0x07, 0x00, --	----	-----	---
DES-CBC3-MD5	0xC0 RSA 0x00, 0x16		RSAA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA		DH	RSAA	3DES-CBC(168)	
SHA1					
ADH-DES-CBC3-SHA	0x00, 0x1B	DH	Nessuno	3DES-CBC(168)	
SHA1					
DES-CBC3-SHA	0x00, 0x0A	RSAA	RSAA	3DES-CBC(168)	
SHA1					

I campi sopra sono:

{nome cifrato sostenibile}  
 {Codice ID cifrato}  
 Kex={scambio di chiavi}  
 Auth={autenticazione}  
 Encrypt={metodo di crittografia simmetrica}  
 MAC={codice di autenticazione del messaggio} {flag di  
 esportazione}

## Sinossi

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.

## Guarda anche

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>

<https://sweet32.info>

## Soluzione

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

## Fattore di rischio

medio

## Punteggio base CVSS v3.0

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

## Punteggio base CVSS v2.0

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

## Riferimenti

CVE CVE-2016-2183

## Informazioni sul plug-in

Pubblicato: 23/11/2009, Modificato: 03/02/2021

## Uscita del plug-in

tcp/5432/postgresql

Cifrature di media potenza (chiave > 64 bit e < 112 bit o 3DES)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	----	-----	---
EDH-RSA-DES-CBC3-SHA SHA1	0x00, 0x16	DH	RSAA	3DES-CBC(168)	
DES-CBC3-SHA SHA1	0x00, 0x0A	RSAA	RSAA	3DES-CBC(168)	

I campi sopra sono:

{nome cifrato sostenibile}

{Codice ID cifrato}

Kex={scambio di chiavi}

Auth={autenticazione}

Encrypt={metodo di crittografia simmetrica}

MAC={codice di autenticazione del messaggio} {flag di  
esportazione}

### Sinossi

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.

Guarda anche

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

### Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

5.0 (CVSS2#E:U/RL:OF/RC:C)

### Riferimenti

OFFERTA

86002

CVE	CVE-2016-2118
XRIF	CERT:813296

Informazioni sul plug-in

---

Pubblicato: 13/04/2016, Modificato: 20/11/2019

Uscita del plug-in

---

tcp/445/cifs

Nessus ha rilevato che la patch Samba Badlock non è stata applicata.

### Sinossi

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.

### Guarda anche

[https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\\_XST\\_ebook.pdf](https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf)

<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

### Soluzione

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

### Fattore di rischio

medio

### Punteggio base CVSS v3.0

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

### Punteggio temporale CVSS v3.0

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### Punteggio base CVSS v2.0

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

### Punteggio temporale CVSS v2.0

3.7 (CVSS2#E:U/RL:OF/RC:C)

### Riferimenti

OFFERTA	9506
OFFERTA	9561
OFFERTA	11604
OFFERTA	33374

OFFERTA	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XRIF	CERT:288308
XRIF	CERT:867593
XRIF	CWE:16
XRIF	CWE: 200

Informazioni sul plug-in

---

Pubblicato: 23/01/2003, Modificato: 12/06/2020

Uscita del plug-in

---

tcp/80/www

Per disabilitare questi metodi, aggiungi le seguenti righe per ogni host virtuale nel tuo file di configurazione:

```
RewriteEngine attivato
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

In alternativa, tieni presente che le versioni Apache 1.3.34, 2.0.55 e 2.2 supportano la disabilitazione nativa del metodo TRACE tramite la direttiva 'TraceEnable'.

Nessus ha inviato la seguente richiesta TRACE:

```
----- taglio ----- TRACE /
Nessus121975629.html HTTP/1.1
Connessione: Chiudi
Host: 192.168.50.101
Pragma: senza cache
User-Agent: Mozilla/4.0 (compatibile; MSIE 8.0; Windows NT 5.1; Trident/4.0) Accetta: image/gif, image/
x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept- Lingua: it
```

Accetta set di caratteri: iso-8859-1,\*,utf-8

```
----- taglio -----
```

e ha ricevuto la seguente risposta dal server remoto:

```
----- taglio ----- HTTP/1.1 200 OK
```

```
Data: Thu, 01 Jun 2023 11:36:26 GMT Server:
Apache/2.2.8 (Ubuntu) DAV/2 Keep-Alive:
timeout=15, max=100 Connessione: Keep-Alive
```

```
Transfer-Encoding: chunked Tipo di
contenuto: message/http
```

```
TRACE /Nessus121975629.html Connessione
HTTP/1.1: Keep-Alive
Host: 192.168.50.101
Pragma: senza cache
Agente utente: Mozilla/4.0 (compatibile; MSIE 8.0; Windows NT 5.1; Trident/4.0) Accetta: image/gif,
image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```



Accetta-Lingua: en  
Accetta set di caratteri: iso-8859-1,\*,utf-8

----- - taglio -----

## Sinossi

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.

Guarda anche

<https://kb.isc.org/docs/cve-2020-8622>

## Soluzione

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Gravità

IO

## Riferimenti

---

CVE	CVE-2020-8622
XRIF	IAVA:2020-A-0385-S

## Informazioni sul plug-in

---

Pubblicato: 27/08/2020, Modificato: 03/06/2021

## Uscita del plug-in

---

udp/53/dns

Versione installata: 9.4.2 Versione  
fissa : 9.11.22, 9.16.6, 9.17.4 o successivo

## 136808 - ISC BIND Denial of Service

### Sinossi

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.

Guarda anche

<https://kb.isc.org/docs/cve-2020-8617>

### Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

3.4 (CVSS2#E:POC/RL:OF/RC:C)

STIG Gravità

IO

Riferimenti

CVE CVE-2020-8617  
XRIF IAVA:2020-A-0217-S

#### Informazioni sul plug-in

---

Pubblicato: 22/05/2020, Modificato: 23/03/2023

#### Uscita del plug-in

---

udp/53/dns

Versione installata: 9.4.2 Versione  
fissa : 9.11.19

### Sinossi

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.

### Guarda anche

<http://www.nessus.org/u?df39b8b3> <http://technet.microsoft.com/en-us/library/cc731957.aspx> <http://www.nessus.org/u?74b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u?a3cac4ea>

### 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.

### Fattore di rischio

medio

### Punteggio base CVSS v3.0

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

### Punteggio temporale CVSS v3.0

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### Punteggio base CVSS v2.0

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

### Punteggio temporale CVSS v2.0

3.7 (CVSS2#E:U/RL:OF/RC:C)

### Informazioni sul plug-in

Pubblicato: 19/01/2012, Modificato: 05/10/2022

Uscita del plug-in

---

tcp/445/cifs

### Sinossi

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.

Guarda anche

<https://tools.ietf.org/html/rfc2487> <https://www.securityfocus.com/archive/1/516901/30/0/threaded>

### Soluzione

Contattare il fornitore per vedere se è disponibile un aggiornamento.

Fattore di rischio

medio

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

3.1 (CVSS2#E:POC/RL:OF/RC:C)

### Riferimenti

OFFERTA	46767
CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XRIF	CERT:555316



Pubblicato: 10/03/2011, Modificato: 06/03/2019

tcp/25/smtp

Nessus ha inviato i seguenti due comandi in un unico pacchetto:

```
STARTTLS\r\nRSET\r\n
```

E il server ha inviato le seguenti due risposte:

```
220 2.0.0 Pronto per iniziare TLS 250  
2.0.0 Ok
```

## 90317 - Algoritmi deboli SSH supportati

### Sinossi

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.

Guarda anche

<https://tools.ietf.org/html/rfc4253#section-6.3>

### Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 04/04/2016, Modificato: 14/12/2016

Uscita del plug-in

tcp/22/ssh

Sono supportati i seguenti algoritmi di crittografia deboli da server a client:

arcfour  
arcfour128  
arcfour256

Sono supportati i seguenti algoritmi di crittografia client-server deboli:

arcfour  
arcfour128  
arcfour256

## 31705 - Suite di cifratura anonime SSL supportate

### Sinossi

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.

### Guarda anche

<http://www.nessus.org/u?3a040ada>

### Soluzione

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

### Fattore di rischio

Basso

### Punteggio base CVSS v3.0

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

### Punteggio temporale CVSS v3.0

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### Punteggio base CVSS v2.0

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

### Punteggio temporale CVSS v2.0

1.9 (CVSS2#E:U/RL:OF/RC:C)

### Riferimenti

OFFERTA	28482
CVE	CVE-2007-1858

### Informazioni sul plug-in

192.168.50.101

Uscita del plug-in

tcp/25/smtp

Di seguito è riportato un elenco di cifrari anonimi SSL supportati dal server TCP remoto:

Crittografie a bassa resistenza (<= chiave a 64 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	---	-----	---
EXP-ADH-DES-CBC-SHA SHA1       esportare	0x00, 0x19	DH(512)	Nessuno	DES-CBC(40)	
EXP-ADH-RC4-MD5 esportare	0x00, 0x17	DH(512)	Nessuno	RC4(40)	MD5
ADH-DES-CBC-SHA SHA1	0x00, 0x1A	DH	Nessuno	DES-CBC(56)	

Cifrature di media potenza (chiave > 64 bit e < 112 bit o 3DES)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	---	-----	---
ADH-DES-CBC3-SHA SHA1	0x00, 0x1B	DH	Nessuno	3DES-CBC(168)	

Cifrature ad alta resistenza (>= chiave a 112 bit)

Nome	Codice	KEX	Aut	Crittografia	MAC
-----	-----	---	---	-----	---
ADH-AES128-SHA SHA1	0x00, 0x34	DH	Nessuno	AES-CBC(128)	
ADH-AES256-SHA SHA1	0x00, 0x3A	DH	Nessuno	AES-CBC(256)	
ADH-RC4-MD5	0x00, 0x18	DH	Nessuno	RC4(128)	MD5

I campi sopra sono:

{nome cifrato sostenibile}  
 {Codice ID cifrato}  
 Kex={scambio di chiavi}  
 Auth={autenticazione}  
 Encrypt={metodo di crittografia simmetrica}  
 MAC={codice di autenticazione del messaggio} {flag di  
 esportazione}

## Sinossi

---

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.

Guarda anche

---

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

## Soluzione

---

Acquista o genera un certificato SSL appropriato per questo servizio.

Fattore di rischio

---

medio

Punteggio base CVSS v3.0

---

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

Punteggio base CVSS v2.0

---

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

Pubblicato: 15/12/2010, Modificato: 27/04/2020

Uscita del plug-in

---

tcp/25/smtp

Il seguente certificato faceva parte della catena di certificati inviata dall'host remoto, ma è scaduto:

| -Soggetto : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Ufficio per Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain

| -Non dopo: 16 aprile 14:07:45 2010 GMT

Il seguente certificato era in cima alla catena di certificati inviata dall'host remoto, ma è firmato da un'autorità di certificazione sconosciuta:

| -Subject : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Ufficio per Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain

| -Emittente : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Office for Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain

## Sinossi

---

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.

Guarda anche

---

<https://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

## Soluzione

---

Acquista o genera un certificato SSL appropriato per questo servizio.

Fattore di rischio

---

medio

Punteggio base CVSS v3.0

---

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

Punteggio base CVSS v2.0

---

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

Pubblicato: 15/12/2010, Modificato: 27/04/2020

Uscita del plug-in

---

tcp/5432/postgresql

Il seguente certificato faceva parte della catena di certificati inviata dall'host remoto, ma è scaduto:

| -Soggetto : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Ufficio per Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain

| -Non dopo: 16 aprile 14:07:45 2010 GMT

Il seguente certificato era in cima alla catena di certificati inviata dall'host remoto, ma è firmato da un'autorità di certificazione sconosciuta:

| -Subject : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Ufficio per Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain

| -Emittente : C=XX/ST=Non esiste nulla di simile al di fuori degli Stati Uniti/L=Ovunque/O=OCOSA/OU=Office for Complicazione di affari altrimenti semplici/CN=ubuntu804-base.localdomain/ E=root@ubuntu804- base.localdomain



## Sinossi

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.

## Fattore di rischio

medio

## Punteggio base CVSS v3.0

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

## Punteggio base CVSS v2.0

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

## Informazioni sul plug-in

Pubblicato: 03/12/2004, Modificato: 03/02/2021

## Uscita del plug-in

tcp/25/smtp

Il certificato SSL è già scaduto:

Soggetto : C=XX, ST=Non esiste nulla di simile al di fuori degli Stati Uniti, L=Ovunque, O=OCOSA, OU=Office for Complication of Altrimenti Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Emittente : C=XX, ST=Non esiste nulla di simile al di fuori degli Stati Uniti, L=Ovunque, O=OCOSA, OU=Office for Complication of Altrimenti Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Non valido prima: Mar 17 14:07:45 2010 GMT Non valido dopo: Apr 16 14:07:45 2010 GMT

## Sinossi

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.

## Fattore di rischio

medio

## Punteggio base CVSS v3.0

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

## Punteggio base CVSS v2.0

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

## Informazioni sul plug-in

Pubblicato: 03/12/2004, Modificato: 03/02/2021

## Uscita del plug-in

tcp/5432/postgresql

Il certificato SSL è già scaduto:

Soggetto : C=XX, ST=Non esiste nulla di simile al di fuori degli Stati Uniti, L=Ovunque, O=OCOSA, OU=Office for Complication of Altrimenti Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Emittente : C=XX, ST=Non esiste nulla di simile al di fuori degli Stati Uniti, L=Ovunque, O=OCOSA, OU=Office for Complication of Altrimenti Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain  
Non valido prima: Mar 17 14:07:45 2010 GMT Non valido dopo: Apr 16 14:07:45 2010 GMT

## 45411 - Certificato SSL con nome host errato

### Sinossi

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.

### Fattore di rischio

medio

### Punteggio base CVSS v3.0

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

### Punteggio base CVSS v2.0

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

### Informazioni sul plug-in

Pubblicato: 03/04/2010, Modificato: 27/04/2020

### Uscita del plug-in

tcp/25/smtp

Le identità conosciute da Nessus sono:

192.168.50.101  
192.168.50.101

Il nome comune nel certificato è:

ubuntu804-base.localdomain

## 45411 - Certificato SSL con nome host errato

### Sinossi

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.

### Fattore di rischio

medio

### Punteggio base CVSS v3.0

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

### Punteggio base CVSS v2.0

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

### Informazioni sul plug-in

Pubblicato: 03/04/2010, Modificato: 27/04/2020

### Uscita del plug-in

tcp/5432/postgresql

Le identità conosciute da Nessus sono:

192.168.50.101  
192.168.50.101

Il nome comune nel certificato è:

ubuntu804-base.localdomain

## 89058 - Vulnerabilità dell'attacco SSL DROWN (decrittografia RSA con crittografia obsoleta e indebolita)

### Sinossi

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 crossprotocol 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.

Guarda anche

<https://drownattack.com/> <https://drownattack.com/drownattack-paper.pdf>

### 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.

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

3.2 (CVSS2#E:U/RL:OF/RC:C)

### Riferimenti