



Essenziali

Metasploitable_Basic

Rapporto generato da Nessus™

Gio, 01 giu 2023 06:56:30 EDT

Nesso

SOMMARIO

Vulnerabilità per host

• 192.168.2.2..... Quattro

Essenziali!

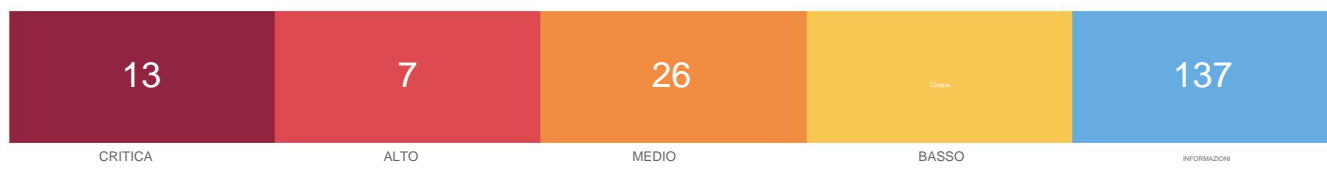
Nesso

Essenziali!

Vulnerabilità per host

Nesso

192.168.2.2



Informazioni sulla scansione

Ora di inizio: Gio 1 giugno 06:33:36 2023

Tempo scaduto: Gio 1 giugno 06:56:29 2023

Informazioni sull'ospite

Nome Netbios: METASPRUTTABILE

IP: 192.168.2.2

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

Vulnerabilità

134862 - Iniezione richiesta connettore Apache Tomcat AJP (Ghostcat)

Sinossi

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

Descrizione

È stata rilevata una vulnerabilità di lettura inclusione del file nel connettore AJP. Un utente malintenzionato remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file di un'applicazione Web da un server vulnerabile.

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?5eafcf70>

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 VPR

9.0

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-NOTA-SFRUTTATA:2022/03/17 |
| XRIF | ID CEA: 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 54 50 2F 31 2E 31 00 00 0F 2F 0x0010: 61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C 0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 0x0040: 00 0 UN 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41
0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00 0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09 0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F età massima=0.....Lu 0x0 0C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74 0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F68

0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73 0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C
64 65 2E 72 65 71 75 65 et.include.reque 0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61 st_uri...1....ja
0x0130: 76 61 78 2E 73 65 72 76 6C 65 7 4 2E 69 6E 63 6C vax.servlet.incl

0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10 0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65 0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65 0x0180: 7 4 5F 70 61 74 68 00 00 00 00 FF

....HTTP/1.1.../asdf/
xxxxx.jsp..localhost.....I

ocalhost..P..... .keep-
alive...A ccept-
Language...en-
US,en;q=0.5.
....0...Accept-E
ncoding...gzip, deflate,
sdch...
Controllo cache...
zilla...Aggiorna richiesta
insicura s...1.....text/h
tml.....localhost...!
javax.servl 0x0110: 65
74 2E 69 6E 63 6C 75

ude.path_info...
/WEB-INF/
web.xml..."javax.servle
t.include.servle t_path.....

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

171340 - Server Web Apache Tomcat SEoL (<= 5.5.x)

Sinossi

Il server Web remoto è obsoleto/non supportato.

Descrizione

Secondo la sua versione, il web server Apache Tomcat è 5.5.x o precedente.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto.

Guarda anche

<https://tomcat.apache.org/>

<https://tomcat.apache.org/tomcat-55-eol.html>

Soluzione

Rimuovere il server Web se non è più necessario.

Fattore di rischio

Alto

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

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

Informazioni sul plug-in

Pubblicato: 10/02/2023, Modificato: 21/03/2023

Uscita del plug-in

tcp/8180/www

URL : <http://192.168.2.2:8180/> Versione installata :
5.5 Fine vita sicurezza : 10 agosto 2011 Tempo dalla fine vita sicurezza
(stimato): 11 anni, 9 mesi, 26 giorni | 4311 giorni totali

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.

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): ----- snip -----
----- root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root) root@ metasfruttabile:/
#
----- taglia -----
```

32314 – Debolezza del generatore di numeri casuali del pacchetto Debian OpenSSH/OpenSSL

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://](http://www.nessus.org/u?f14f4224)

www.nessus.org/u?f14f4224

Soluzione

Considerare indovicabile 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 VPR

7.4

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

32321 – Debolezza del generatore di numeri casuali del pacchetto Debian OpenSSH/OpenSSL (verifica SSL)

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 impostare un attacco man in the middle.

Guarda anche

<http://www.nessus.org/u?107f9bdc> [http://](http://www.nessus.org/u?f14f4224)

www.nessus.org/u?f14f4224

Soluzione

Considerare indovicabile 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 VPR

7.4

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

32321 – Debolezza del generatore di numeri casuali del pacchetto Debian OpenSSH/OpenSSL (verifica SSL)

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 impostare un attacco man in the middle.

Guarda anche

<http://www.nessus.org/u?107f9bdc> [http://](http://www.nessus.org/u?f14f4224)

www.nessus.org/u?f14f4224

Soluzione

Considerare indovicabile 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 VPR

7.4

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

11356 - Divulgazione di informazioni sulla condivisione esportata NFS

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 e un utente malintenzionato potrebbe essere in grado di sfruttarla per leggere (ed eventualmente scrivere) file sull'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 VPR

5.9

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 / :

- .
- ..

-bin-

avvio

-cdrom-dev

-eccetera

- casa -

initrd

- initrd.img - lib -

perso+trovato -

media

-mnt

- nohup.out - opt

- proc -

root - sbin

-srv

-sys-

tmp

-usr

-var

- vmlinuz

20007 - Rilevamento del protocollo SSL versione 2 e 3

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 i servizi e i client interessati.

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 applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del 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.nessus.org/u?5d15ba70 <https://>

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

[html/rfc7507](https://tools.ietf.org/html/rfc7507) <https://tools.ietf.org/html/>

[rfc7568](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 | | ARS (512) | RSAA | RC2-CBC(40) | MD5 |
| esportare | | | | | |
| EXP-RC4-MD5 | | ARS (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 (>= chiavi 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) | |
| SHA1 esportare | | | | | |
| EDH-RSA-DES-CBC-SHA | | DH | RSAA | DES-CBC(56) | SHA |
| [...] | | | | | |

20007 - Rilevamento del protocollo SSL versione 2 e 3

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 i servizi e i client interessati.

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 applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del 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.nessus.org/u?5d15ba70 <https://>

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

[html/rfc7507](https://tools.ietf.org/html/rfc7507) <https://tools.ietf.org/html/>

[rfc7568](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 (>= chiavi 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}

33850 - Rilevamento versione non supportata del sistema operativo Unix

Sinossi

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

Descrizione

In base al numero di versione auto-rapportato, 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.

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 IAVA: 0001-A-0502

XRIF IAV: 0001-A-0648

Informazioni sul plug-in

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

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>

46882 - Rilevamento backdoor IRCd irreale

Sinossi

Il server IRC remoto contiene una backdoor.

Descrizione

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.

Guarda anche

<https://seclists.org/fulldisclosure/2010/Jun/277> <https://seclists.org/fulldisclosure/2010/Jun/284> <http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Soluzione

Scarica nuovamente il software, verificalo utilizzando i checksum MD5/SHA1 pubblicati e reinstallalo.

Fattore di rischio

Critico

Punteggio VPR

7.4

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 | 40820 |
| CVE | CVE-2010-2075 |

Sfruttabile con

CANVAS (vero) Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 14/06/2010, Modificato: 11/04/2022

Uscita del plug-in

tcp/6697/irc

Il server IRC remoto è in esecuzione come:

uid=0(radice) gid=0(radice)

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 con 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 sfruttarla per assumere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password complessa.

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".

10203 - Rilevamento servizio rexecd

Sinossi

Il servizio rexecd è in esecuzione sull'host remoto.

Descrizione

Il servizio rexecd è in esecuzione sull'host 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.

Fattore di rischio

Critico

Punteggio VPR

6.7

Punteggio base CVSS v2.0

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

Riferimenti

CVE CVE-1999-0618

Informazioni sul plug-in

Pubblicato: 31/08/1999, Modificato: 13/08/2018

Uscita del plug-in

tcp/512/rexecd

136769 - Downgrade del servizio ISC BIND / DoS riflesso

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 un rinvio risposta.

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 VPR

5.2

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

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

42256 - Condivisioni NFS leggibili in tutto il mondo

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:

/*

42873 - Suite di cifratura a media resistenza SSL supportate (SWEET32)

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 media potenza. Nessus considera media forza 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://](https://sweet32.info)

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 VPR

6.1

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 |
| DES-CBC3-MD5 | 0x07, 0x00, 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} | | | | | |

42873 - Suite di cifratura a media resistenza SSL supportate (SWEET32)

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 media potenza. Nessus considera media forza 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 VPR

6.1

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 | 0x00, 0x16 | DH | RSAA | 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} | | | | | |

90509 - Vulnerabilità al blocco di Samba**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 impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questo difetto 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 di sicurezza sensibili 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 VPR

6.7

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)

192.168.2.2

Riferimenti

| | |
|---------|---------------|
| OFFERTA | 86002 |
| CVE | CVE-2016-2118 |
| XRIF | CERT:813296 |

Informazioni sul plug-in

Pubblicato: 13 aprile 2016, Modificato: 20 novembre 2019

Uscita del plug-in

tcp/445/cifs

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

10205 - Rilevamento servizio rlogin

Sinossi

Il servizio rlogin è in esecuzione sull'host remoto.

Descrizione

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono trasmessi tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttarlo per sniffare accessi e password. accessi scarsamente autenticati senza password Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile aggirare l'autenticazione.

Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura ai file in accessi completi tramite i file .rhosts o rhosts.equiv.

Soluzione

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

Fattore di rischio

Alto

Punteggio VPR

6.7

Punteggio base CVSS v2.0

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

Riferimenti

CVE CVE-1999-0651

Sfruttabile con

Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 30/08/1999, Modificato: 11/04/2022

Uscita del plug-in

tcp/513/rlogin

10245 - Rilevamento servizio rsh

Sinossi

Il servizio rsh è in esecuzione sull'host remoto.

Descrizione

Il servizio rsh è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono trasmessi tra il client e il server rsh in chiaro. Un utente malintenzionato man-in-the-middle può sfruttarlo per sniffare accessi e password. accessi scarsamente autenticati senza password Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile aggirare l'autenticazione.

Infine, rsh è un modo semplice per trasformare l'accesso in scrittura ai file in accessi completi tramite i file .rhosts o rhosts.equiv.

Soluzione

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

Fattore di rischio

Alto

Punteggio VPR

6.7

Punteggio base CVSS v2.0

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

Riferimenti

CVE CVE-1999-0651

Sfruttabile con

Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 22/08/1999, Modificato: 11/04/2022

Uscita del plug-in

tcp/514/rsh