192.168.49.101

9	5	23	5	87
CRITICA	ALTO	MEDIO	BASSO	INFORMAZIONI

Informazioni sulla scansione

Ora di inizio:	Gio Feb 23 08:41:03 2023 Gio
Tempo scaduto:	Feb 23 09:01:04 2023

Informazioni sull'ospite

Nome Netbios:	METASPRUTTABILE
IP:	192.168.49.101
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 JSP (JavaServer Pages) 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?5eafcf70

Soluzione

Aggiorna la configurazione A JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o 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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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: 13/02/2023

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 61 73 64   . . . . HTTP/1.1.../
0x0010:  66 2F 78 78 78 78 78 2E 6A 73 70 00 00                     asdf/xxxxx.jsp..
```

```
0x0020:     09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C 6F 63 61 6C  . localhost.....l
0x0030:     68 6F 73 74 00 00 50 00 00 09 A0 06 00 0A 6B 65 65 70 2D     ocalhost..P.....
0x0040:     61 6C 0605 69 0 76 00 0A 6B 65 65 70 65 70 74 2d 4c 61 6e     . . mantenere in vita...A
0x0050:     67 75 61 67 65 00 00 0e 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30  ccept-Lingua..
0x0060:     2e 35 00 a0 08 00 01 30 00 00 0f 41 63 63 65 70 74 2d 45 6e   . en-US,en;q=0.5.
0x0070:     63 6f 64 69 6e 67 00 00 13 67 7a 69 70 2c 20 64 65 66 6c 61   . . . . 0...Accept-E
0x0080:     74 65 2C 20 73 64 63 68 00 00 0d 43 61 63 68 65 2d 43 6f 6e  ncoding...gzip,
0x0090:     74 72 6f 6c 00 00 09 6d 61 78 2d 61 61 65 3D 30 00 A0 0E 00   sgonfiare, sdch...
0x00A0:     07 4D 6F 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D     Controllo cache...
0x00B0:     49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 730 0 10 300 10      max-età=0.....Lu
0x00C0:     300 74 74 00 09 74 65 78 74 2f 68 74 6d 6c 00 a0 0b 00 09     zilla...Aggiorna-
0x00D0:      6c 6f 63 61 6c 68 6f 73 74 00 0a 00 21 6a 61 76 61 78 2e 73   Richiesta insicura
0x00E0:     65 72 76 6c 65 74 2e 69 6e 63 6c 6c 64 65 2E 72 65 71 75 65  s...1.....testo/h
0x00F0:     73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61 76 61 78 2E   tml.....localhos
0x0100:     73 65 72 76 6C 65 74 2E 69 6E63 6c 75 64 65 2e 70 61 74 68    t...!javax.servl
0x0110:     5f 69 6e 66 6f 00 00 10 2f 57 45 42 2d 49 4e 46 2f 77 65 62   et.include.reque
0x0120:     2e 78 6d 6c 00 0a 00 22 6a 61 76 61 78 2e 73 65 72 76 6c 65  st_uri...1....ja
0x0130:     74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65 74 5F 70 61   vax.servlet.incl
0x0140:     74 68 00 00 00 00 FF                                          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 [...]

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://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)

CVSS v2.0 TemporaSl core

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 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)

CVSS v2.0 TemporaSl core

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 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)

CVSS v2.0 TemporaSl core

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. 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

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 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.

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/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        RSA 3DES-CBC(168)             MD5

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

    Nome                    Codice          KEX         Aut       Crittografia          MAC
    ----------------------  ----------      ---         ----      --------------------  ---
    - - RC4-MD5                             RSAA        - - - - RSA 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 Esportazione SHA1           DH(512)     RSAA      DES-CBC(40)

    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 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.

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/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
    RSA-DES-CBC3-SHA                             DH      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    RSA         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-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: 2023/02/07

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".
```

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 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 a cui si fa riferimento 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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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

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 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
- - - - DES-CBC3-MD5	0x07, 0x00, 0xC0	RSA	RSA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	DH	RSA	3DES-CBC(168)	SHA1
ADH-DES-CBC3-SHA	0x00, 0x1B	DH	Nessuno	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	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 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	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 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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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.

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

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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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 corretta: 9.11.22, 9.16.6, 9.17.4 o successiva

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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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: 12/09/2022

Uscita del plug-in

udp/53/dns

Versione installata: 9.4.2
Versione fissa: 9.11.19

57608 - Firma SMB non richiesta

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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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

52611 - Servizio SMTP STARTTLS Iniezione di comandi in testo normale

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)

CVSS v2.0 TemporaSl core

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

Informazioni sul plug-in

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

Uscita del plug-in

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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	28482
CVE	CVE-2007-1858

Informazioni sul plug-in

Pubblicato: 28/03/2008, Modificato: 03/02/2021

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	0x00, 0x19	- - DH(512)	Nessuno	DES-CBC(40)	Esportazione SHA1	
EXP-ADH-RC4-MD5	0x00, 0x17	DH(512)	Nessuno	RC4(40)	MD5	esportare
ADH-DES-CBC-SHA	0x00, 0x1A	DH	Nessuno	DES-CBC(56)	SHA1	

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

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

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

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

51192 - Il certificato SSL non può essere considerato attendibile

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-themiddle 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)

Informazioni sul plug-in

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:

|-Subject : 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/ 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=Office for
 Complication of Altrimenti Simple Affairs/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
 Complication of Altrimenti Simple Affairs/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-themiddle 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)

Informazioni sul plug-in

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:

|-Subject : 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/ 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=Office for Complication of Altrimenti Simple Affairs/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 Complication of Altrimenti Simple Affairs/CN=ubuntu804-base.localdomain/ E=root@ ubuntu804-base.localdomain

15901 - Scadenza certificato SSL

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

15901 - Scadenza certificato SSL

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:

192.168.49.101
192.168.49.101

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:

192.168.49.101
192.168.49.101

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)

CVSS v3.0 TemporaSl core

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)

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	83733
CVE	CVE-2016-0800
XRIF	CERT:583776

Informazioni sul plug-in

Pubblicato: 01/03/2016, Modificato: 20/11/2019

Uscita del plug-in

tcp/25/smtp

L'host remoto è interessato da SSL DROWN e supporta le seguenti suite di cifratura vulnerabili:

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

Nome	Codice	KEX	Aut	Crittografia	MAC
EXP-RC2-CBC-MD5 esportare	0x04, 0x00, 0x80	RSA(512)	RSAA	RC2-CBC(40)	MD5
EXP-RC4-MD5 esportare	0x02, 0x00, 0x80	RSA(512)	RSAA	RC4(40)	MD5

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

Nome	Codice	KEX	Aut	Crittografia	MAC
- - RC4-MD5	0x01, 0x00, 0x80	RSA		RSA 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}

65821 - Suite di cifratura SSL RC4 supportate (Bar Mitzvah)

Sinossi

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 attaccante 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.

Guarda anche

https://www.rc4nomore.com/ http://

www.nessus.org/u?ac7327a0 http://cr.yp.to/

talks/2013.03.12/slides.pdf http://www.isg.

rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

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.

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)

CVSS v3.0 TemporaSl core

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

Punteggio base CVSS v2.0

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

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	58796
OFFERTA	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Informazioni sul plug-in

Pubblicato: 2013/04/05, Modificato: 2021/02/03

Uscita del plug-in

tcp/25/smtp

Elenco delle suite di cifratura RC4 supportate dal server remoto:

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

Nome	Codice	KEX	Aut	Crittografia	MAC
EXP-RC4-MD5 esportare	0x02, 0x00, 0x80	RSA(512)	RSAA	RC4(40)	MD5
EXP-ADH-RC4-MD5 esportare	0x00, 0x17	DH(512)	Nessuno	RC4(40)	MD5
EXP-RC4-MD5 esportare	0x00, 0x03	RSA(512)	RSAA	RC4(40)	MD5

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

Nome	Codice	KEX	Aut	Crittografia	MAC
RC4-MD5	0x01, 0x00, 0x80	RSA	RSA	RC4(128)	MD5
ADH-RC4-MD5	0x00, 0x18	DH	Nessuno	RC4(128)	MD5
RC4-MD5	0x00, 0x04	RSAA	RSAA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	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}

65821 - Suite di cifratura SSL RC4 supportate (Bar Mitzvah)

Sinossi

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 attaccante 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.

Guarda anche

https://www.rc4nomore.com/ http://

www.nessus.org/u?ac7327a0 http://cr.yp.to/

talks/2013.03.12/slides.pdf http://www.isg.

rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

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.

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)

CVSS v3.0 TemporaSl core

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

Punteggio base CVSS v2.0

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

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	58796
OFFERTA	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Informazioni sul plug-in

Pubblicato: 2013/04/05, Modificato: 2021/02/03

Uscita del plug-in

tcp/5432/postgresql

Elenco delle suite di cifratura RC4 supportate dal server remoto:

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

Nome	Codice	KEX	Aut	Crittografia	MAC
--- RC4-SHA	0x00, 0x05	RSAA	RSA	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}

57582 - Certificato autofirmato SSL

Sinossi

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-themiddle 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.

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)

Informazioni sul plug-in

Pubblicato: 17/01/2012, Modificato: 14/06/2022

Uscita del plug-in

tcp/25/smtp

```
Il seguente certificato è stato trovato in cima alla catena di certificati
inviata dall'host remoto, ma è autofirmato e non è stato trovato
nell'elenco delle autorità di certificazione conosciute:

|-Subject : 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/ E=root@ ubuntu804-
 base.localdomain
```

57582 - Certificato autofirmato SSL

Sinossi

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-themiddle 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.

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)

Informazioni sul plug-in

Pubblicato: 17/01/2012, Modificato: 14/06/2022

Uscita del plug-in

tcp/5432/postgresql

```
Il seguente certificato è stato trovato in cima alla catena di certificati
inviata dall'host remoto, ma è autofirmato e non è stato trovato
nell'elenco delle autorità di certificazione conosciute:

|-Subject : 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/ E=root@ ubuntu804-
 base.localdomain
```

26928 - Suite di cifratura deboli SSL supportate

Sinossi

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.

Guarda anche

http://www.nessus.org/u?6527892d

Soluzione

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

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 base CVSS v2.0

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

Riferimenti

XRIF	CWE: 326
XRIF	CWE: 327
XRIF	CWE:720
XRIF	CWE:753
XRIF	CWE:803
XRIF	CWE:928
XRIF	CWE:934

Informazioni sul plug-in

Pubblicato: 2007/10/08, Modificato: 2021/02/03

Uscita del plug-in

Ecco l'elenco delle crittografie SSL deboli supportate dal server remoto:

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

Nome	Codice	KEX	Aut	Crittografia	MAC	
EXP-RC2-CBC-MD5	0x04, 0x00, 0x80	RSA(512)	RSAA	RC2-CBC(40)	MD5	esportare
EXP-RC4-MD5	0x02, 0x00, 0x80	RSA(512)	RSAA	RC4(40)	MD5	esportare
EXP-EDH-RSA-DES-CBC-SHA	0x00, 0x14	DH(512)	RSAA	DES-CBC(40)		Esportazione SHA1
EDH-RSA-DES-CBC-SHA	0x00, 0x15	DH	RSAA	DES-CBC(56)		SHA1
EXP-ADH-DES-CBC-SHA	0x00, 0x19	DH(512)	Nessuno	DES-CBC(40)		Esportazione SHA1
EXP-ADH-RC4-MD5	0x00, 0x17	DH(512)	Nessuno	RC4(40)	MD5	esportare
ADH-DES-CBC-SHA	0x00, 0x1A	DH	Nessuno	DES-CBC(56)		SHA1
EXP-DES-CBC-SHA	0x00, 0x08	RSA(512)	RSAA	DES-CBC(40)		Esportazione SHA1
EXP-RC2-CBC-MD5	0x00, 0x06	RSA(512)	RSAA	RC2-CBC(40)	MD5	esportare
EXP-RC4-MD5	0x00, 0x03	RSA(512)	RSAA	RC4(40)	MD5	esportare
DES-CBC-SHA	0x00, 0x09	RSAA	RSAA	DES-CBC(56)		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}

81606 - SSL/TLS EXPORT_RSA <= suite di cifratura a 512 bit supportate (FREAK)

Sinossi

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 attaccante man-in-the-middle potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di cifratura EXPORT_RSA (ad es. CVE-2015-0204). Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

Guarda anche

https://www.smacktls.com/#freak https://

www.openssl.org/news/secadv/20150108.txt http://

www.nessus.org/u?b78da2c4

Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v2.0

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

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	71936
CVE	CVE-2015-0204
XRIF	CERT:243585

Informazioni sul plug-in

Pubblicato: 04/03/2015, Modificato: 03/02/2021

Uscita del plug-in

Suite di crittografia EXPORT_RSA supportate dal server remoto:

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

Nome	Codice	KEX	Aut	Crittografia	MAC
EXP-DES-CBC-SHA	0x00, 0x08	RSA(512)	RSAA	DES-CBC(40)	
Esportazione SHA1					
EXP-RC2-CBC-MD5	0x00, 0x06	RSA(512)	RSAA	RC2-CBC(40)	MD5
esportare					
EXP-RC4-MD5	0x00, 0x03	RSA(512)	RSAA	RC4(40)	MD5
esportare					

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}

78479 - SSLv3 Padding Oracle su vulnerabilità di crittografia legacy ridotta (POODLE)

Sinossi

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.

Guarda anche

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

www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/

html/draft -ietf-tls-downgrade-scsv-00

Soluzione

Disabilita SSLv3.

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

CVSS v3.0 TemporaSl core

5.9 (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)

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	70574
CVE	CVE-2014-3566
XRIF	CERT:577193

Informazioni sul plug-in

Pubblicato: 15/10/2014, Modificato: 12/06/2020

Uscita del plug-in

tcp/25/smtp

Nessus ha stabilito che il server remoto supporta SSLv3 con almeno una suite di crittografia CBC, indicando che questo server è vulnerabile.

Sembra che TLSv1 o più recente sia supportato sul server. Tuttavia, il meccanismo SCSV di fallback non è supportato, consentendo il "rollback" delle connessioni a SSLv3.

78479 - SSLv3 Padding Oracle su vulnerabilità di crittografia legacy ridotta (POODLE)

Sinossi

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.

Guarda anche

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

www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/

html/draft -ietf-tls-downgrade-scsv-00

Soluzione

Disabilita SSLv3.

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

CVSS v3.0 TemporaSl core

5.9 (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)

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	70574
CVE	CVE-2014-3566
XRIF	CERT:577193

Informazioni sul plug-in

Pubblicato: 15/10/2014, Modificato: 12/06/2020

Uscita del plug-in

tcp/5432/postgresql

Nessus ha stabilito che il server remoto supporta SSLv3 con almeno una suite di crittografia CBC, indicando che questo server è vulnerabile.

Sembra che TLSv1 o più recente sia supportato sul server. Tuttavia, il meccanismo SCSV di fallback non è supportato, consentendo il "rollback" delle connessioni a SSLv3.

104743 - Rilevamento protocollo TLS versione 1.0

Sinossi

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.

Guarda anche

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 22/11/2017, Modificato: 31/03/2020

Uscita del plug-in

tcp/25/smtp

```
TLSv1 è abilitato e il server supporta almeno una crittografia.
```

104743 - Rilevamento protocollo TLS versione 1.0

Sinossi

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.

Guarda anche

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Soluzione

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

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 22/11/2017, Modificato: 31/03/2020

Uscita del plug-in

tcp/5432/postgresql

TLSv1 è abilitato e il server supporta almeno una crittografia.

70658 - Crittografia in modalità CBC del server SSH abilitata

Sinossi

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.

Fattore di rischio

Basso

Punteggio base CVSS v2.0

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

CVSS v2.0 TemporaSl core

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

Riferimenti

OFFERTA	32319
CVE	CVE-2008-5161
XRIF	CERT:958563
XRIF	CWE: 200

Informazioni sul plug-in

Pubblicato: 28/10/2013, Modificato: 30/07/2018

Uscita del plug-in

tcp/22/ssh

Sono supportati i seguenti algoritmi Cipher Block Chaining (CBC) da client a server:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
pesce palla-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Sono supportati i seguenti algoritmi Cipher Block Chaining (CBC) da server a client:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
pesce palla-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

153953 - Algoritmi di scambio di chiavi deboli SSH abilitati

Sinossi

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.

Guarda anche

http://www.nessus.org/u?b02d91cd https://
datatracker.ietf.org/doc/html/rfc8732

Soluzione

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

Fattore di rischio

Basso

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 13/10/2021, Modificato: 13/10/2021

Uscita del plug-in

tcp/22/ssh

Sono abilitati i seguenti algoritmi di scambio di chiavi deboli:

diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1

71049 - Algoritmi MAC deboli SSH abilitati

Sinossi

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.

Fattore di rischio

Basso

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 22/11/2013, Modificato: 14/12/2016

Uscita del plug-in

tcp/22/ssh

```
Sono supportati i seguenti algoritmi MAC (Message Authentication Code) da client a
server:

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

Sono supportati i seguenti algoritmi MAC (Message Authentication Code) da server a
client:

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

83738 - SSL/TLS EXPORT_DHE <= suite di crittografia di esportazione a 512 bit supportate (logjam)

Sinossi

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.

Guarda anche

https://weakdh.org/

Soluzione

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

Fattore di rischio

Basso

Punteggio base CVSS v3.0

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

CVSS v3.0 TemporaSl core

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

Punteggio base CVSS v2.0

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

CVSS v2.0 TemporaSl core

2.2 (CVSS2#E:U/RL:ND/RC:C)

Riferimenti

OFFERTA	74733
CVE	CVE-2015-4000
XRIF	CEA-ID:CEA-2021-0004

Informazioni sul plug-in

Pubblicato: 21/05/2015, Modificato: 05/12/2022

Uscita del plug-in

tcp/25/smtp

EXPORT_DHE suite di crittografia supportate dal server remoto:

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

Nome	Codice	KEX	Aut	Crittografia	MAC	
EXP-EDH-RSA-DES-CBC-SHA	Esportazione SHA1	0x00, 0x14	DH(512)	RSAA	DES-CBC(40)	
EXP-ADH-DES-CBC-SHA		0x00, 0x19	DH(512)	Nessuno	DES-CBC(40)	
Esportazione SHA1						
EXP-ADH-RC4-MD5		0x00, 0x17	DH(512)	Nessuno	RC4(40)	MD5
esportare						

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}

10407 - Rilevamento server X

Sinossi

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).

Fattore di rischio

Basso

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 12/05/2000, Modificato: 05/03/2019

Uscita del plug-in

tcp/6000/x11

Versione X11: 11.0