metasploitable_Basic_2

Rapporto generato da Nessus™ Ven, 02 Jun 2023 13:08:58 CEST

SOMMARIO

Vulnerabilità per host

Vulnerabilità per host

192.168.2.2

CRITICA	ALTO	MEDIO	BASSO	INFORMAZIONI
7	6	25	4	116

Informazioni sulla scansione

Ora di inizio:	Ven 2 giu 12:51:28 2023
Tempo scaduto:	Ven 2 giu 13:08:57 2023

Informazioni sull'ospite

Nome Netbios:	METASPRUTTABILE
IP:	192.168.2.2
Sistema operativo:	Linux Kernel 2.6 su Ubuntu 8.04 (resistente)

Vulnerabilità

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 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 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 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://

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 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

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 esportare		RSA(512)	RSAA	RC2-CBC(40)	MD5
EXP-RC4-MD5 esportare		RSA(512)	RSAA	RC4(40)	MD5

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

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

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

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

I campi sopra sono:

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

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

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

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

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

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

I campi sopra sono:

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

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: 2023/05/18

Uscita del plug-in

TCP/0

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

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

46882 - UnrealIRCd Rilevamento backdoor

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)

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 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:

/var/condividi/pubblico *

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 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	RSAA	3DES-CBC(168)	MD5
EDH-RSA-DES-CBC3-SHA	0x00, 0x16	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 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 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, che esiste 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 disattivazione 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)

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.

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 passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttarlo per sniffare accessi e password. Inoltre, potrebbe consentire 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. In alternativa, disabilita questo servizio e usa invece SSH.

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