Vulnerability assessment macchina Metasploitable

Sun, 27 Aug 2023 05:00:30 EDT

Summary

CRITICAL	HIGH	MEDIUM	LOW	INFO
14	10	34	13	161

Scan Information

Start time:	Sun Aug 27 04:39:26 2023
End time:	Sun Aug 27 05:00:29 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.100
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Dettaglio vulnerabilità

20007 (2) - SSL Version 2 and 3 Protocol Detection

Sinossi

Il servizio remoto cripta il traffico utilizzando un protocollo con vulnerabilità note.

Descrizione

Il servizio remoto accetta connessioni crittografate tramite SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di padding insicuro con i cifrari CBC.

- Schemi di rinegoziazione e ripristino della sessione non sicuri.

Un aggressore può sfruttare queste falle per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più recente del protocollo supportata (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser Web lo implementano in modo non sicuro, consentendo a un aggressore di eseguire il downgrade della connessione (come nel caso di POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di applicazione prevista da PCI DSS v3.1, qualsiasi versione di SSL non soddisfa la definizione di "crittografia forte" del PCI SSC.

See Also

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 suite di cifratura approvate) o superiore.

Fattore di rischio

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

32321 (2) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Sinossi

Il certificato SSL remoto utilizza una chiave debole.

Descrizione

Il certificato remoto x509 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 ad un pacchettizzatore Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un uomo nell'attacco centrale.

See Also

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

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

Soluzione

Tutto il materiale crittografico generato sull'host remoto deve essere considerato decrittabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN deve essere rigenerato.

Fattore di Rischio

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 29179
CVE CVE-2008-0166
XREF CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

11356 (1) - NFS Exported Share Information Disclosure

Sinossi

It is possible to access NFS shares on the remote host.

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 questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Fattore di Rischio

Critical

CVSS v2.0 Base Score

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

References

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

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output

192.168.50.100 (udp/2049/rpc-nfs)

32314 (1) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Sinossi

Le chiavi dell'host remoto SSH sono deboli.

Descrizione

La chiave host SSH remota 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 alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un aggressore può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.

See Also

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

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

Soluzione

Tutto il materiale crittografico generato sull'host remoto deve essere considerato decrittabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN deve essere rigenerato.

Fattore di Rischio

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

192.168.50.100 (tcp/22/ssh)

33850 (1) - Unix Operating System Unsupported Version Detection

Sinossi

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

Descrizione

Secondo il numero di versione dichiarato, 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

Aggiornare a una versione del sistema operativo Unix attualmente supportata.

Fattore di Rischio

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0502
XREF IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2023/07/07

Plugin Output

192.168.50.100 (tcp/0)

46882 (1) - UnrealIRCd Backdoor Detection

-

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.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277

https://seclists.org/fulldisclosure/2010/Jun/284

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Soluzione

Scaricare nuovamente il software, verificarlo utilizzando le checksum MD5 / SHA1 pubblicate e reinstallarlo.

Fattore di Rischio

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 40820
CVE CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/6667/irc)

51988 (1) - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione

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

Fattore di Rischio

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/1524/wild_shell)

61708 (1) - VNC Server 'password' Password

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 effettuare il login utilizzando l'autenticazione VNC e una password "password". Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Soluzione

Secure the VNC service with a strong password.

Fattore di Rischio

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

192.168.50.100 (tcp/5900/vnc)

70728 (1) - Apache PHP-CGI Remote Code Execution

Sinossi

Il server Web remoto contiene una versione di PHP che consente l'esecuzione di codice arbitrario.

Descrizione

L'installazione di PHP sul server web remoto contiene una falla che potrebbe consentire a un utente remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Ciò potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un crash del sistema, ecc.

Soluzione

Aggiornare a PHP 5.3.13 / 5.4.3 o successivo.

Fattore di Rischio

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827
XREF	EDB-ID:29290
XREF	EDB-ID:29316
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2013/11/01, Modified: 2023/04/25

Plugin Output

192.168.50.100 (tcp/80/www)

125855 (1) - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Sinossi

Il server Web remoto ospita un'applicazione PHP affetta da una vulnerabilità SQLi.

Descrizione

Secondo il numero di versione dichiarato, l'applicazione phpMyAdmin ospitata sul server Web remoto è precedente alla versione 4.8.6. Pertanto, è affetta da una vulnerabilità SQL injection (SQLi) presente nella funzione designer di phpMyAdmin. È quindi affetta da una vulnerabilità SQL injection (SQLi) presente in una funzione di progettazione di phpMyAdmin. Un aggressore remoto non autenticato può sfruttare questa vulnerabilità per iniettare o manipolare query SQL nel database back-end, con conseguente divulgazione o manipolazione di dati arbitrari.
Si noti che Nessus non ha tentato di sfruttare questi problemi, ma si è basato solo sul numero di versione auto-riportato dell'applicazione.

See Also

http://www.nessus.org/u?c9d7fc8c

Soluzione

Aggiornare a phpMyAdmin versione 4.8.6 o successiva.
In alternativa, applicare le patch indicate negli avvisi del fornitore.

Fattore di Rischio

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 108617
CVE CVE-2019-11768

Plugin Information

Published: 2019/06/13, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

134862 (1) - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Sinossi

Sull'host remoto è in ascolto un connettore AJP vulnerabile.

Descrizione

È stata riscontrata una vulnerabilità nella lettura/inclusione di file in AJP connector. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

See Also

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/Soluzioni/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

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

Fattore di Rischio

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

Published: 2020/03/24, Modified: 2023/07/17

Plugin Output

192.168.50.100 (tcp/8009/ajp13)

171340 (1) - Apache Tomcat SEoL (<= 5.5.x)

Sinossi

Sull'host remoto è installata una versione non supportata di Apache Tomcat.

Descrizione

Secondo la sua versione, Apache Tomcat è inferiore o uguale a 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

See Also

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

Soluzione

Aggiornare a una versione di Apache Tomcat attualmente supportata.

Fattore di Rischio

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2023/02/10, Modified: 2023/06/13

Plugin Output

192.168.50.100 (tcp/8180/www)

42873 (2) - SSL Medium Strength Cipher Suites Supported (SWEET32)

-

Sinossi

Il servizio remoto supporta l'uso di cifrari SSL medium strength.

Descrizione

L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia medium strength. Nessus considera medium strength qualsiasi crittografia che utilizzi chiavi di lunghezza minima di 64 bit e inferiore a 112 bit, oppure che utilizzi la suite di crittografia 3DES.

Si noti che è molto più facile aggirare la crittografia medium strength se l'attaccante si trova sulla stessa rete fisica.

See Also

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

https://sweet32.info

Soluzione

Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari medium strength.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

10205 (1) - rlogin Service Detection

-

Sinossi

The rlogin service is running on the remote host.

Descrizione

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client rlogin e il server in chiaro. Un attaccante man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, può consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'indovinare il numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (compreso l'hijacking ARP su una rete locale), potrebbe essere possibile bypassare l'autenticazione.
Infine, rlogin è un modo semplice per trasformare l'accesso alla scrittura dei file in login completi attraverso i file .rhosts o rhosts.equiv.

Soluzione

Commentare la riga "login" in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare invece SSH.

Fattore di Rischio

High

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/30, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/513/rlogin)

10245 (1) - rsh Service Detection

Sinossi

Il servizio rsh è in esecuzione sull'host remoto.

Descrizione

Il servizio rsh è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rsh in chiaro. Un attaccante man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, può consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'indovinare il numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (compreso l'hijacking ARP su una rete locale), potrebbe essere possibile bypassare l'autenticazione.
Infine, rsh è un modo semplice per trasformare l'accesso alla scrittura dei file in login completi attraverso i file .rhosts o rhosts.equiv.

Soluzione

Commentare la riga "rsh" in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare invece SSH.

Fattore di Rischio

High

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/22, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/514/rsh)

19704 (1) - TWiki 'rev' Parameter Arbitrary Command Execution

Sinossi

Il server Web remoto ospita un'applicazione CGI affetta da una vulnerabilità nell'esecuzione di comandi arbitrari.

Descrizione

La versione di TWiki in esecuzione sull'host remoto consente a un utente malintenzionato di manipolare l'input del parametro "rev" per eseguire comandi shell arbitrari sull'host remoto con i privilegi dell'utente id del server web.

See Also

http://www.nessus.org/u?c70904f3

Soluzione

Applicare l'hotfix appropriato indicato nell'advisory del fornitore.

Fattore di Rischio

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.2 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 14834
CVE CVE-2005-2877

Exploitable With

Metasploit (true)

Plugin Information

Published: 2005/09/15, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

36171 (1) - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

Sinossi

Il server Web remoto contiene un'applicazione PHP affetta da una vulnerabilità di esecuzione del codice.

Descrizione

Lo script di configurazione incluso nella versione di phpMyAdmin installata sull'host remoto non sanifica correttamente l'input fornito dall'utente prima di utilizzarlo per generare un file di configurazione per l'applicazione. Questa versione è affetta dalle seguenti vulnerabilità:

- Lo script di configurazione inserisce il nome del server verboso non sanificato in un commento in stile C durante la generazione del file di configurazione.

- Un utente malintenzionato può salvare dati arbitrari nel file di configurazione generato alterando il valore del parametro "textconfig" durante una richiesta POST a config.php.

See Also

https://www.tenable.com/security/research/tra-2009-02

http://www.phpmyadmin.net/home_page/security/PMASA-2009-4.php

Soluzione

Aggiornare a phpMyAdmin 3.1.3.2. In alternativa, applicare le patch indicate nell'advisory del progetto.

Fattore di Rischio

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	34526
CVE	CVE-2009-1285
XREF	TRA:TRA-2009-02
XREF	SECUNIA:34727
XREF	CWE:94

Plugin Information

Published: 2009/04/16, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

42256 (1) - NFS Shares World Readable

Sinossi

Il server NFS remoto esporta condivisioni leggibili in tutto il mondo.

Descrizione

Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a hostname, IP o intervallo IP).

See Also

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

Soluzione

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2020/05/05

Plugin Output

192.168.50.100 (tcp/2049/rpc-nfs)

59088 (1) - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

Sinossi

Il server web remoto contiene una versione di PHP che consente l'esecuzione di codice arbitrario.

Descrizione

L'installazione di PHP sul server web remoto contiene una falla che potrebbe consentire a un utente remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Ciò potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un crash del sistema, ecc.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

http://www.php.net/ChangeLog-5.php#5.4.3

http://www.nessus.org/u?80589ce8

https://www-304.ibm.com/support/docview.wss?uid=swg21620314

Soluzione

Se si utilizza Lotus Foundations, aggiornare il sistema operativo Lotus Foundations alla versione 1.2.2b o successiva.
Altrimenti, aggiornare a PHP 5.3.13 / 5.4.3 o successivo.

Fattore di Rischio

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
XREF	CERT:520827
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	EDB-ID:18834

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/05/14, Modified: 2022/03/28

Plugin Output

192.168.50.100 (tcp/80/www)

90509 (1) - Samba Badlock Vulnerability

Sinossi

Un server SMB in esecuzione sull'host remoto è affetto dalla vulnerabilità Badlock.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da una falla, nota come Badlock, presente nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali Remote Procedure Call (RPC). Un utente malintenzionato che sia in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare il declassamento del livello di autenticazione, consentendo l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili di sicurezza nel database Active Directory (AD) o la disabilitazione di servizi critici.

See Also

http://badlock.org

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

Soluzione

Aggiornare a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

192.168.50.100 (tcp/445/cifs)

136769 (1) - ISC BIND Service Downgrade / Reflected DoS

Sinossi

Il server dei nomi remoto è affetto da vulnerabilità Service Downgrade / Reflected DoS.

Descrizione

Secondo la versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è affetta da vulnerabilità di downgrade delle prestazioni e DoS riflesso. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di fetch che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.
Un aggressore remoto non autenticato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

See Also

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

Soluzione

Aggiornare alla versione di ISC BIND indicata nell'avviso del fornitore.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

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

Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

Plugin Output

192.168.50.100 (udp/53/dns)

15901 (2) - SSL Certificate Expiry

Sinossi

Il certificato SSL del server remoto è già scaduto.

Descrizione

Questo plugin controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sul target e segnala se sono già scaduti.

Soluzione

Acquistare o generare un nuovo certificato SSL per sostituire quello esistente.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

45411 (2) - SSL Certificate with Wrong Hostname

Sinossi

Il certificato SSL per questo servizio è di un altro host.

Descrizione

L'attributo "commonName" (CN) del certificato SSL presentato per questo servizio è relativo a una macchina diversa.

Soluzione

Acquistare o generare un certificato SSL adeguato per questo servizio.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

51192 (2) - SSL Certificate Cannot Be Trusted

Sinossi

Il certificato SSL per questo servizio non è attendibile.

Descrizione

Il certificato X.509 del server non è attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena di fiducia può essere interrotta, come indicato di seguito:

- In primo luogo, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un'autorità di certificazione pubblica nota. Ciò può verificarsi sia quando il vertice della catena è un certificato non riconosciuto e autofirmato, sia quando mancano i certificati intermedi che collegherebbero il vertice della catena di certificati a un'autorità di certificazione pubblica nota.

- In secondo luogo, la catena di certificati può contenere un certificato non valido al momento della scansione. Ciò può verificarsi sia quando la scansione avviene prima di una delle date "notBefore" del certificato, sia dopo una delle date "notAfter" del certificato.

- In terzo luogo, la catena del certificato può contenere una firma che non corrisponde alle informazioni del certificato o che non può essere verificata. Le firme errate possono essere corrette facendo rifirmare il certificato con la firma errata dal suo emittente. Le firme che non possono essere verificate 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 della catena rende più difficile per gli utenti verificare l'autenticità e l'identità del server web. Ciò potrebbe facilitare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

See Also

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

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

Soluzione

Acquistare o generare un certificato SSL adeguato per questo servizio.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

57582 (2) - SSL Self-Signed Certificate

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

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

Soluzione

Acquistare o generare un certificato SSL adeguato per questo servizio.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

-

Sinossi

Il servizio remoto supporta l'uso del cifrario RC4.

Descrizione

L'host remoto supporta l'uso di RC4 in una o più suite di cifratura.
Il cifrario RC4 ha un difetto nella generazione di un flusso pseudocasuale di byte, per cui un'ampia varietà di piccole distorsioni viene introdotta nel flusso, riducendone la casualità.

Se il testo in chiaro viene crittografato ripetutamente (ad esempio, i cookie HTTP) e un aggressore è in grado di ottenere molti (ad esempio, decine di milioni) testi cifrati, l'aggressore può essere in grado di ricavare il testo in chiaro.

See Also

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 dei cifrari RC4. Considerare l'utilizzo di TLS 1.2 con suite AES-GCM, a seconda del supporto del browser e del server web.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

85582 (2) - Web Application Potentially Vulnerable to Clickjacking

Sinossi

Il server Web remoto potrebbe non riuscire a mitigare una classe di vulnerabilità delle applicazioni Web.

Descrizione

Il server Web remoto non imposta un'intestazione di risposta X-Frame-Options o un'intestazione di risposta Content-Security-Policy "frame-ancestors" in tutte le risposte di contenuto. Ciò potrebbe esporre il sito a un attacco di clickjacking o UI redress, in cui un aggressore può indurre un utente a fare clic su un'area della pagina vulnerabile diversa da quella che l'utente percepisce come pagina. Questo può portare l'utente a eseguire transazioni fraudolente o dannose.

X-Frame-Options è stato proposto da Microsoft come metodo per mitigare gli attacchi di clickjacking ed è attualmente supportato da tutti i principali fornitori di browser.

Content-Security-Policy (CSP) è stato proposto dal W3C Web Application Security Working Group, con un crescente supporto da parte di tutti i principali fornitori di browser, come metodo per mitigare il clickjacking e altri attacchi. La direttiva "frame-ancestors" limita le fonti che possono incorporare la risorsa protetta.

Si noti che, sebbene le intestazioni di risposta X-Frame-Options e Content-Security-Policy non siano le uniche mitigazioni per il clickjacking, attualmente sono i metodi più affidabili che possono essere rilevati attraverso l'automazione. Pertanto, questo plugin potrebbe produrre falsi positivi se vengono utilizzate altre strategie di mitigazione (ad esempio, JavaScript frame-busting) o se la pagina non esegue alcuna transazione sensibile alla sicurezza.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

Soluzione

Restituisce l'intestazione HTTP X-Frame-Options o Content-Security-Policy (con la direttiva "frame-ancestors") con la risposta della pagina.
Questo impedisce che il contenuto della pagina venga reso da un altro sito quando si utilizzano i tag HTML frame o iframe.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

References

XREF CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

192.168.50.100 (tcp/80/www)

192.168.50.100 (tcp/8180/www)

104743 (2) - TLS Version 1.0 Protocol Detection

Sinossi

Il servizio remoto cripta il traffico utilizzando una versione precedente di TLS.

Descrizione

Il servizio remoto accetta connessioni crittografate con TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 attenuano questi problemi, ma le versioni più recenti di TLS, come la 1.2 e la 1.3, sono progettate contro questi difetti e dovrebbero essere utilizzate ogni volta che è possibile.
A partire dal 31 marzo 2020, gli endpoint che non sono 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 completamente disabilitato 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 suscettibili di exploit noti.

See Also

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

Soluzione

Abilitare il supporto per TLS 1.2 e 1.3 e disabilitare il supporto per TLS 1.0.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

11213 (1) - HTTP TRACE / TRACK Methods Allowed

Sinossi

Le funzioni di debug sono abilitate sul server web remoto.

Descrizione

Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni al server Web.

See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

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

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

Soluzione

Disabilitare questi metodi HTTP. Per ulteriori informazioni, consultare l'output del plugin.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567

CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

192.168.50.100 (tcp/80/www)

11229 (1) - Web Server info.php / phpinfo.php Detection

Sinossi

Il server Web remoto contiene uno script PHP che è soggetto a un attacco di divulgazione di informazioni.

Descrizione

Molti tutorial per l'installazione di PHP indicano all'utente di creare un file PHP che richiami la funzione PHP "phpinfo()" a scopo di debug. Anche diverse applicazioni PHP possono includere un file di questo tipo. Accedendo a tale file, un aggressore remoto può scoprire una grande quantità di informazioni sul server Web remoto, tra cui :

- Il nome utente dell'utente che ha installato PHP e se è un utente SUDO.
- L'indirizzo IP dell'host.
- La versione del sistema operativo.
- La versione del server web.
- La directory principale del server web.
- Informazioni di configurazione sull'installazione PHP remota.

Soluzione

Rimuovere i file interessati.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2003/02/12, Modified: 2022/06/01

Plugin Output

192.168.50.100 (tcp/80/www)

11411 (1) - Backup Files Disclosure

Sinossi

È possibile recuperare i backup dei file dal server web remoto.

Descrizione

Aggiungendo vari suffissi (ad esempio .old, .bak, ~, ecc.) ai nomi di vari file sull'host remoto, sembra possibile recuperarne il contenuto, il che potrebbe portare alla divulgazione di informazioni sensibili.

See Also

http://www.nessus.org/u?8f3302c6

Soluzione

Assicuratevi che i file non contengano informazioni sensibili, come le credenziali di connessione a un database, ed eliminate o proteggete i file che non devono essere accessibili.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2003/03/17, Modified: 2023/07/10

Plugin Output

192.168.50.100 (tcp/80/www)

12085 (1) - Apache Tomcat Default Files

Sinossi

Il server web remoto contiene file predefiniti.

Descrizione

Sul server Apache Tomcat remoto sono installati la pagina di errore predefinita, la pagina di indice predefinita, JSP di esempio e/o servlet di esempio. Questi file devono essere rimossi perché potrebbero aiutare un utente malintenzionato a scoprire informazioni sull'installazione Tomcat remota o sull'host stesso.

See Also

http://www.nessus.org/u?4cb3b4dd

https://www.owasp.org/index.php/Securing_tomcat

Soluzione

Eliminare la pagina indice predefinita e rimuovere il JSP e le servlet di esempio. Seguire le istruzioni di Tomcat o OWASP per sostituire o modificare la pagina di errore predefinita.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/03/02, Modified: 2019/08/12

Plugin Output

192.168.50.100 (tcp/8180/www)

26928 (1) - SSL Weak Cipher Suites Supported

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.

See Also

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

Soluzione

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

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

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

Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

31705 (1) - SSL Anonymous Cipher Suites Supported

Sinossi

Il servizio remoto supporta l'uso di cifrari SSL anonimi.

Descrizione

L'host remoto supporta l'uso di cifrari SSL anonimi. Se da un lato questo consente all'amministratore di impostare un servizio che cripta il traffico senza dover generare e configurare certificati SSL, dall'altro non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.
L'host remoto supporta l'uso di cifrari SSL anonimi. Se da un lato questo consente all'amministratore di impostare un servizio che cripta il traffico senza dover generare e configurare certificati SSL, dall'altro 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.

See Also

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

Soluzione

Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari deboli.

Fattore di Rischio

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 28482
CVE CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

35806 (1) - Tomcat Sample App cal2.jsp 'time' Parameter XSS

Sinossi

Il server Web remoto contiene un'applicazione JSP affetta da una vulnerabilità cross-site scripting.

Descrizione

Il server Web remoto include un'applicazione JSP di esempio, "cal2.jsp", che non riesce a sanificare l'input fornito dall'utente prima di utilizzarlo per generare contenuto dinamico. Un aggressore remoto non autenticato può sfruttare questo problema per iniettare codice HTML o script arbitrario nel browser di un utente, che verrà eseguito nel contesto di sicurezza del sito interessato.

See Also

https://www.securityfocus.com/archive/1/501538/30/0/threaded

http://tomcat.apache.org/security-6.html

http://tomcat.apache.org/security-5.html

http://tomcat.apache.org/security-4.html

Soluzione

Aggiornare alla versione 4.1.40 / 5.5.28 / 6.0.20 di Apache Tomcat.In alternativa, applicare la patch appropriata indicata nell'advisory del fornitore o disinstallare l'applicazione web Tomcat examples.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-2009-0781
XREF	CWE:79

Plugin Information

Published: 2009/03/09, Modified: 2021/01/19

Plugin Output

192.168.50.100 (tcp/8180/www)

36083 (1) - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)

Sinossi

Il server Web remoto contiene uno script PHP che presenta diversi problemi.

Descrizione

La versione di phpMyAdmin installata sull'host remoto non riesce a sanificare l'input fornito dall'utente al parametro "file_path" dello script "bs_disp_as_mime_type.php" prima di utilizzarlo per leggere un file e riportarlo in HTML generato dinamicamente. Un aggressore remoto non autenticato potrebbe essere in grado di sfruttare questo problema per leggere file arbitrari, eventualmente da host terzi, o per iniettare intestazioni HTTP arbitrarie nelle risposte inviate a utenti terzi.
Si noti che l'applicazione è anche affetta da diversi altri problemi, sebbene Nessus non li abbia effettivamente verificati.

See Also

https://www.phpmyadmin.net/security/PMASA-2009-1/

Soluzione

Aggiornare a phpMyAdmin 3.1.3.1 o applicare la patch indicata nell'advisory del progetto.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 34253
XREF SECUNIA:34468

Plugin Information

Published: 2009/04/03, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

40984 (1) - Browsable Web Directories

Sinossi

Some directories on the remote web server are browsable.

Descrizione

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Soluzione

Assicuratevi che le directory sfogliabili non facciano trapelare informazioni riservate o diano accesso a risorse sensibili. Inoltre, utilizzare restrizioni di accesso o disabilitare l'indicizzazione delle directory per quelle che lo fanno.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

192.168.50.100 (tcp/80/www)

42263 (1) - Unencrypted Telnet Server

Sinossi

Il server Telnet remoto trasmette il traffico in chiaro.

Descrizione

L'host remoto sta eseguendo un server Telnet su un canale non criptato.
L'uso di Telnet su un canale non crittografato è sconsigliato, poiché login, password e comandi vengono trasferiti in chiaro. Ciò consente a un aggressore remoto, man-in-the-middle, di origliare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e di modificare il traffico scambiato tra client e server.
SSH è preferibile a Telnet in quanto protegge le credenziali dalle intercettazioni e può trasmettere flussi di dati aggiuntivi, come una sessione X11.

Soluzione

Disattivare il servizio Telnet e utilizzare invece SSH.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

192.168.50.100 (tcp/23/telnet)

46803 (1) - PHP expose_php Information Disclosure

Sinossi

La configurazione di PHP sull'host remoto consente la divulgazione di informazioni sensibili.

Descrizione

L'installazione di PHP sul server remoto è configurata in modo da consentire la divulgazione di informazioni potenzialmente sensibili a un utente malintenzionato attraverso un URL speciale. Tale URL attiva un Easter egg integrato in PHP stesso.
È probabile che esistano altri Easter egg di questo tipo, ma Nessus non li ha verificati.

See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

Soluzione

Nel file di configurazione di PHP, php.ini, impostare il valore di 'expose_php' su 'Off' per disabilitare questo comportamento. Riavviare il demone del server web per rendere effettiva questa modifica.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/06/03, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

49142 (1) - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
-

Sinossi

Il server Web remoto contiene un'applicazione PHP che presenta una vulnerabilità cross-site scripting.

Descrizione

Lo script di configurazione incluso nella versione di phpMyAdmin installata sull'host remoto non sanifica correttamente l'input fornito dall'utente nel campo "verbose server name".

Un aggressore remoto potrebbe sfruttare questo problema inducendo l'utente a eseguire codice script arbitrario.

See Also

https://www.tenable.com/security/research/tra-2010-02

https://www.phpmyadmin.net/security/PMASA-2010-7/

Soluzione

Upgrade to phpMyAdmin 3.3.7 or later.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2010-3263
XREF	TRA:TRA-2010-02
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800

XREF CWE:801
XREF CWE:809
XREF CWE:811
XREF CWE:864
XREF CWE:900
XREF CWE:928
XREF CWE:931
XREF CWE:990

Plugin Information

Published: 2010/09/08, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

51425 (1) - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

Sinossi

Il server Web remoto ospita uno script PHP che è soggetto a un attacco cross- site scripting.

Descrizione

La versione di phpMyAdmin non riesce a convalidare i tag BBcode inseriti dall'utente nel parametro "error" dello script "error.php" prima di utilizzarlo per generare HTML dinamico.
Un utente malintenzionato potrebbe essere in grado di sfruttare questo problema per iniettare codice HTML o script arbitrario nel browser di un utente e farlo eseguire nel contesto di sicurezza del sito interessato. Ad esempio, potrebbe essere utilizzato per far visualizzare una pagina con testo arbitrario e un link a un sito esterno.

See Also

https://www.phpmyadmin.net/security/PMASA-2010-9/

Soluzione

Aggiornare a phpMyAdmin 3.4.0-beta1 o successivo.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	45633
CVE	CVE-2010-4480
XREF	EDB-ID:15699
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2011/01/06, Modified: 2022/04/11

Plugin Output

192.168.50.100 (tcp/80/www)

52611 (1) - SMTP Service STARTTLS Plaintext Command Injection

Sinossi

Il servizio di posta remota consente l'iniezione di comandi in testo semplice durante la negoziazione di un canale di comunicazione crittografato.

Descrizione

Il servizio SMTP remoto contiene una falla software nella sua implementazione STARTTLS che potrebbe consentire a un aggressore remoto non autenticato di iniettare comandi durante la fase di protocollo plaintext che verranno eseguiti durante la fase di protocollo ciphertext.
Uno sfruttamento riuscito potrebbe consentire a un aggressore di rubare l'e-mail della vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

See Also

https://tools.ietf.org/html/rfc2487

https://www.securityfocus.com/archive/1/516901/30/0/threaded

Soluzione

Contattare il fornitore per verificare se è disponibile un aggiornamento.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	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
XREF	CERT:555316

Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

Plugin Output

192.168.50.100 (tcp/25/smtp)

57608 (1) - SMB Signing not required

Sinossi

La firma non è richiesta sul server SMB remoto.

Descrizione

La firma non è richiesta sul server SMB remoto. Un aggressore remoto non autenticato può sfruttare questa situazione per condurre attacchi man-in-the-middle contro il server SMB.

See Also

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

Applicare la firma dei messaggi nella configurazione dell'host. In Windows, si trova nell'impostazione di criterio "Server di rete Microsoft: Firma digitale delle comunicazioni (sempre)". Su Samba, l'impostazione si chiama "firma del server". Per ulteriori dettagli, consultare i link "Vedi anche".

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

192.168.50.100 (tcp/445/cifs)

81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Sinossi

L'host remoto supporta una serie di cifrari deboli.

Descrizione

L'host remoto supporta suite di cifratura EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato è in grado di determinare un modulo RSA a 512 bit in un breve lasso di tempo.
Un utente malintenzionato potrebbe essere in grado di declassare la sessione per utilizzare suite di cifratura EXPORT_RSA (ad esempio, CVE-2015-0204). Pertanto, si raccomanda di rimuovere il supporto per le suite di cifratura deboli.

See Also

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

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	71936
CVE	CVE-2015-0204
XREF	CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

192.168.50.100 (tcp/25/smtp)

89058 (1) - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Sinossi

L'host remoto potrebbe essere affetto da una vulnerabilità che consente a un aggressore remoto di decifrare potenzialmente il traffico TLS catturato.

Descrizione

L'host remoto supporta SSLv2 e pertanto potrebbe essere affetto da una vulnerabilità che consente un attacco cross-protocol Bleichenbacher padding oracle noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità è dovuta a una falla nell'implementazione di Secure Sockets Layer Version 2 (SSLv2) e consente di decifrare il traffico TLS catturato. Un attaccante man-in-the-middle può sfruttare questo aspetto per decifrare la connessione TLS utilizzando il traffico catturato in precedenza e una crittografia debole insieme a una serie di connessioni appositamente create a un server SSLv2 che utilizza la stessa chiave privata.

See Also

https://drownattack.com/

https://drownattack.com/drown-attack-paper.pdf

Soluzione

Disattivare SSLv2 e le suite di crittografia di grado export. Assicurarsi che le chiavi private non vengano utilizzate in nessun caso con il software del server che supporta le connessioni SSLv2.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	83733
CVE	CVE-2016-0800
XREF	CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

Plugin Output

192.168.50.100 (tcp/25/smtp)

90317 (1) - SSH Weak Algorithms Supported

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 il cifrario Arcfour o nessun cifrario. La RFC 4253 sconsiglia l'uso di Arcfour a causa di un problema di chiavi deboli.

See Also

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

Soluzione

Contact the vendor or consult product documentation to remove the weak ciphers.

Fattore di Rischio

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

192.168.50.100 (tcp/22/ssh)

136808 (1) - ISC BIND Denial of Service

Sinossi

Il server dei nomi remoto è affetto da una vulnerabilità di fallimento dell'asserzione.

Descrizione

Nelle versioni 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 di ISC BIND esiste una vulnerabilità di tipo denial of service (DoS). Un attaccante remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente creato, per causare l'interruzione della risposta del servizio.
Si noti che Nessus non ha testato questo problema, ma si è basato solo sul numero di versione auto-riportato dell'applicazione.

See Also

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

Soluzione

Aggiornare alla release patchata più vicina alla versione attuale di BIND.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

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

Plugin Information

Published: 2020/05/22, Modified: 2023/03/23

Plugin Output

192.168.50.100 (udp/53/dns)

139915 (1) - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Sinossi

The remote name server is affected by a denial of service vulnerability.

Descrizione

Secondo il numero di versione dichiarato, 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 affetta da una vulnerabilità di tipo denial service (DoS) dovuta a un errore di asserzione quando si tenta di verificare una risposta troncata a una richiesta firmata da TSIG. Pertanto, è affetto da una vulnerabilità di negazione del servizio (DoS) dovuta a un errore di asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata TSIG. Un aggressore autenticato e remoto può sfruttare questo problema inviando una risposta troncata a una richiesta firmata TSIG per attivare un fallimento dell'asserzione, causando l'uscita del server.
Si noti che Nessus non ha testato questo problema, ma si è basato solo sul numero di versione auto-riportato dell'applicazione.

See Also

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

Soluzione

Aggiornare a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

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

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

192.168.50.100 (udp/53/dns)

26194 (2) - Web Server Transmits Cleartext Credentials

Sinossi

Il server Web remoto potrebbe trasmettere le credenziali in chiaro.

Descrizione

Il server Web remoto contiene diversi campi modulo HTML contenenti un input di tipo "password" che trasmettono le loro informazioni a un server Web remoto in chiaro.
Un aggressore che intercetta il traffico tra il browser Web e il server può ottenere login e password di utenti validi.

Soluzione

Assicurati che ogni forma sensibile trasmetta contenuti tramite HTTPS.

Fattore di Rischio

Low

CVSS v2.0 Base Score

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

References

XREF CWE:522
XREF CWE:523
XREF CWE:718
XREF CWE:724
XREF CWE:928
XREF CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

192.168.50.100 (tcp/80/www)

192.168.50.100 (tcp/8180/www)

42057 (2) - Web Server Allows Password Auto-Completion

Sinossi

L'attributo 'autocomplete' non è disabilitato nei campi password.

Descrizione

Il server web remoto contiene almeno un campo modulo HTML che ha un input di tipo 'password' dove 'autocomplete' non è impostato su 'off'.
Anche se questo non rappresenta un rischio per questo server web di per sé, significa che gli utenti che utilizzano i moduli interessati possono avere le loro credenziali salvate nei loro browser, che a sua volta potrebbe portare a una perdita di riservatezza se qualcuno di loro utilizza un host condiviso o se la sua macchina è compromessa ad un certo punto.

Soluzione

Aggiungere l'attributo 'autocomplete=off' a questi campi per impedire ai browser di memorizzare nella cache le credenziali.

Fattore di Rischio

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

192.168.50.100 (tcp/80/www)

192.168.50.100 (tcp/8180/www)

78479 (2) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Sinossi

È possibile ottenere informazioni sensibili dall'host remoto con servizi abilitati SSL/TLS.

Descrizione

L'host remoto è interessato da un man-in-the-middle (MitM) vulnerabilità divulgazione delle informazioni noto come BARBONCINO. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittazione dei messaggi crittografati utilizzando cifrari a blocchi in modalità di concatenamento dei blocchi cifrati (CBC).
Gli aggressori MitM possono decifrare 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 sulle connessioni SSL 3.0 appena create.Finché un client e un servizio supportano entrambi SSLv3, una connessione può essere 'rollback' a SSLv3, anche se TLSv1 o più recente è supportato dal client e dal servizio.Il meccanismo TLS Fallback SCSV previene gli attacchi di rollback della versione senza impattare i client legacy; tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disattivare SSLv3 immediatamente dovrebbero attivare questo meccanismo.Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. Disabilitare SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

See Also

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

Disattivare SSLv3.
I servizi che devono supportare SSLv3 dovrebbero abilitare il meccanismo TLS Fallback SCSV fino a quando SSLv3 può essere disabilitato.

Fattore di Rischio

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

Plugin Output

192.168.50.100 (tcp/25/smtp)

192.168.50.100 (tcp/5432/postgresql)

10407 (1) - X Server Detection

Sinossi

Un server X11 è in ascolto sull'host remoto.

Descrizione

L'host remoto sta eseguendo 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.
Dal momento che il traffico X11 non è cifrato, è possibile per un attaccante di intercettare la connessione.

Soluzione

Limita l'accesso a questa porta. Se la funzione client/server X11 non è usata, disabilita completamente il supporto TCP in X11 (-nolisten tcp).

Fattore di Rischio

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2000/05/12, Modified: 2019/03/05

Plugin Output

192.168.50.100 (tcp/6000/x11)

34850 (1) - Web Server Uses Basic Authentication Without HTTPS

Sinossi

Il server web remoto sembra trasmettere le credenziali in chiaro.

Descrizione

Il server web remoto contiene pagine web protette da 'Basic'
autenticazione su testo libero.
Un malintenzionato che intercetta il traffico potrebbe ottenere login e password di utenti validi.

Soluzione

Assicurarsi che l'autenticazione HTTP venga trasmessa tramite HTTPS.

Fattore di Rischio

Low

CVSS v2.0 Base Score

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

References

XREF CWE:319
XREF CWE:928
XREF CWE:930
XREF CWE:934

Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

Plugin Output

192.168.50.100 (tcp/8180/www)

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Sinossi

Il server SSH è configurato per usare Cipher Block Chaining.

Descrizione

Il server SSH è configurato per supportare la crittografia CBC (Cipher Block Chaining). Ciò può consentire a un utente malintenzionato di recuperare il messaggio in chiaro dal testo cifrato.
Si noti che questo plugin 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 cifrata in modalità CBC e attivare la crittografia in modalità cifratura CTR o GCM.

Fattore di Rischio

Low

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

192.168.50.100 (tcp/22/ssh)

71049 (1) - SSH Weak MAC Algorithms Enabled

Sinossi

Il server SSH remoto è configurato per consentire algoritmi MD5 e MAC a 96 bit.

Descrizione

Il server SSH remoto è configurato per consentire algoritmi MD5 o MAC a 96 bit, entrambi considerati deboli.
Si noti che questo plugin controlla solo le opzioni del server SSH, e non controlla per 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

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

192.168.50.100 (tcp/22/ssh)

83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

-

Sinossi

L'host remoto supporta un insieme di cifrari deboli.

Descrizione

L'host remoto supporta le suite di cifratura EXPORT_DHE con chiavi inferiori o uguali a 512 bit. Attraverso la crittanalisi, una terza parte può trovare il segreto condiviso in un breve lasso di tempo. Un attaccante man-in-the medio potrebbe essere in grado di declassare la sessione per usare le suite di cifratura EXPORT_DHE. Pertanto, si consiglia di rimuovere il supporto per le suite di cifratura deboli.

See Also

https://weakdh.org/

Soluzione

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

Fattore di Rischio

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	74733
CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/21, Modified: 2022/12/05

Plugin Output

192.168.50.100 (tcp/25/smtp)

83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

-

Sinossi

L'host remoto consente connessioni SSL/TLS con uno o più moduli Diffie-Hellman inferiori o uguali a 1024 bit

.

Descrizione

L'host remoto consente connessioni SSL/TLS con uno o più moduli Diffie-Hellman inferiori o uguali a 1024 bit. Attraverso la crittanalisi, una terza parte può essere in grado di trovare il segreto condiviso in un breve lasso di tempo (a seconda delle dimensioni del modulo e delle risorse dell'attaccante). Questo può consentire a un utente malintenzionato di recuperare il testo in chiaro o potenzialmente violare l'integrità delle connessioni.

See Also

https://weakdh.org/

Soluzione

Riconfigurare il servizio per utilizzare un modulo Diffie-Hellman unico di 2048 bit o superiore.

Fattore di Rischio

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	74733
CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2022/12/05

Plugin Output

192.168.50.100 (tcp/25/smtp)

153953 (1) - SSH Weak Key Exchange Algorithms Enabled

Sinossi

Il server SSH remoto è configurato per consentire algoritmi di scambio chiavi deboli.

Descrizione

Il server SSH remoto è configurato per consentire algoritmi di scambio 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 include:

Diffie-Hellman-gruppo-scambio-sha1
Diffie-Hellman-Group1-sha1
gss-Gex-sha1-*
gss-Group1-sha1-*
gss-Group14-sha1-*
rsa1024-sha1

Si noti che questo plugin controlla solo le opzioni del server SSH, e non controlla per le versioni software vulnerabili.

See Also

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

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

192.168.50.100 (tcp/22/ssh)