Second Scan Metasploit

Report generated by Nessus™ Thu, 01 Jun 2023 09:59:31 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
32	61	99	12	144

Scan Information

Start time: Thu Jun 1 08:31:05 2023
End time: Thu Jun 1 09:59:30 2023

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.101
MAC Address: 08:00:27:30:46:AB
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

57603 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow

Synopsis

Il server Web remoto è interessato da una vulnerabilità di overflow del buffer.

Description

Secondo il suo banner auto-riportato, la versione di Apache 2.2.x in esecuzione sull'host remoto è precedente a 2.2.13. In quanto tale, include una versione in bundle della libreria Apache Portable Runtime (APR) che contiene un file difetto in 'apr_palloc()' che potrebbe causare un overflow dell'heap.

Si noti che il server Apache HTTP stesso non passa dimensioni fornite dall'utente non sanificate a questa funzione, quindi it potrebbe essere attivato solo tramite qualche altra applicazione che lo utilizza in modo vulnerabile.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache 2.2.13 or later.

Risk Factor

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 temporale CVSS v3.0

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

Punteggio VPR

6.7

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

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

Riferimenti

OFFERTA	35949
CVE	CVE-2009-2412
XRIF	CWE: 189

Informazioni sul plug-in

Pubblicato: 19/01/2012, Modificato: 29/06/2018

Uscita del plug-in

tcp/80/www

```
Fonte della versione     : Server: Apache/2.2.8 (Ubuntu) DAV/2
Versione installata: 2.2.8 Versione
fissa                    : 2.2.13
```

45004 - Apache 2.2.x < 2.2.15 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità

Descrizione

Secondo il suo banner, la versione di Apache 2.2.x in esecuzione sull'host remoto è precedente alla 2.2.15. È, quindi, potenzialmente affetto da molteplici vulnerabilità:

- È possibile un attacco di iniezione del prefisso di rinegoziazione TLS. (CVE-2009-3555)

- Il modulo 'mod_proxy_ajp' restituisce il codice di stato errato se incontra un errore che porta il server back-end in uno stato di errore. (CVE-2010-0408)

- Il 'mod_isapi' tenta di scaricare 'ISAPI.dll' quando incontra vari stati di errore che potrebbero lasciare i call-back in uno stato indefinito. (CVE-2010-0425)

- Un difetto nel codice di processo della sotto-richiesta principale può portare a informazioni riservate da una richiesta gestita dal thread sbagliato se viene utilizzato un ambiente multi-thread. (CVE-2010-0434)

- Aggiunto il modulo 'mod_reqtimeout' per mitigare gli attacchi di Slowloris. (CVE-2007-6750)

Guarda anche

http://httpd.apache.org/security/vulnerabilities_22.html

https://bz.apache.org/bugzilla/show_bug.cgi?id=48359

https://archive.apache.org/dist/httpd/CHANGES_2. 2.15

Soluzione

Aggiorna ad Apache versione 2.2.15 o successiva.

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 temporale CVSS v3.0

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

Punteggio VPR

9.0

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	21865
OFFERTA	36935
OFFERTA	38491
OFFERTA	38494
OFFERTA	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XRIF	Secunia:38776
XRIF	CWE: 200
XRIF	CWE: 310

Sfruttabile con

Core Impact (vero)

Informazioni sul plug-in

Pubblicato: 20/10/2010, Modificato: 15/11/2018

Uscita del plug-in

tcp/80/www

```
Fonte della versione     : Server: Apache/2.2.8 (Ubuntu) DAV/2
Versione installata: 2.2.8 Versione
fissa                    : 2.2.15
```

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

Secondo il suo banner, la versione di Apache in esecuzione sull'host remoto è 2.2.x precedente alla 2.2.33-dev o 2.4.x precedente alla 2.4.26. È, quindi, affetto dalle seguenti vulnerabilità:

- Esiste una vulnerabilità di bypass dell'autenticazione dovuta a moduli di terze parti che utilizzano la funzione ap_get_basic_auth_pw() al di fuori della fase di autenticazione. Un utente malintenzionato remoto non autenticato può sfruttarlo per aggirare i requisiti di autenticazione. (CVE-2017-3167)

- Esiste un difetto di dereferenziazione del puntatore NULL dovuto a chiamate di moduli di terze parti alla funzione mod_ssl ap_hook_process_connection() durante una richiesta HTTP a una porta HTTPS. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare una condizione di negazione del servizio. (CVE-2017-3169)

- Esiste un difetto di dereferenziazione del puntatore NULL in mod_http2 che viene attivato durante la gestione di una richiesta HTTP/2 appositamente predisposta. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare una condizione di negazione del servizio. Si noti che questa vulnerabilità non riguarda 2.2.x.

(CVE-2017-7659)

- Esiste un errore di lettura fuori limite nella funzione ap_find_token() a causa di una gestione impropria delle sequenze di intestazione. Un utente malintenzionato remoto non autenticato può sfruttarlo, tramite una sequenza di intestazione appositamente predisposta, per causare una condizione di negazione del servizio.

(CVE-2017-7668)

- Esiste un errore di lettura fuori limite in mod_mime a causa di una gestione impropria delle intestazioni di risposta Content-Type. Un utente malintenzionato remoto non autenticato può sfruttarlo, tramite un'intestazione di risposta Content-Type appositamente predisposta, per causare una condizione di negazione del servizio o la divulgazione di informazioni riservate. (CVE-2017-7679)

Si noti che Nessus non ha testato questi problemi, ma ha invece fatto affidamento solo sul numero di versione dell'applicazione segnalato dall'utente.

Guarda anche

https://archive.apache.org/dist/httpd/CHANGES_2.2.32 https://

archive.apache.org/dist/httpd/CHANGES_2.4.26 https://

httpd.apache.org/security/vulnerabilities_22.html https

https://httpd.apache.org/security/vulnerabilities_24.html

Soluzione

Aggiorna alla versione Apache 2.2.33-dev / 2.4.26 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

6.7

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

Riferimenti

OFFERTA	99132
OFFERTA	99134
OFFERTA	99135
OFFERTA	99137
OFFERTA	99170
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7659
CVE	CVE-2017-7668
CVE	CVE-2017-7679

Informazioni sul plug-in

Pubblicato: 22/06/2017, Modificato: 11/04/2022

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.2.33
```

101787 - Apache 2.2.x < 2.2.34 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

Secondo il suo banner, la versione di Apache in esecuzione sull'host remoto è la 2.2.x precedente alla 2.2.34. È, quindi, affetto dalle seguenti vulnerabilità:

- Esiste una vulnerabilità di bypass dell'autenticazione in httpd a causa di moduli di terze parti che utilizzano la funzione ap_get_basic_auth_pw() al di fuori della fase di autenticazione. Un utente malintenzionato remoto non autenticato può sfruttarlo per aggirare i requisiti di autenticazione. (CVE-2017-3167)

- Esiste una vulnerabilità Denial of Service in httpd a causa di un difetto di dereferenziazione del puntatore NULL che viene attivato quando un modulo di terze parti chiama la funzione mod_ssl ap_hook_process_connection() durante una richiesta HTTP a una porta HTTPS. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare una condizione di negazione del servizio. (CVE-2017-3169)

- Esiste una vulnerabilità di negazione del servizio in httpd a causa di un errore di lettura fuori limite nella funzione ap_find_token() che viene attivato durante la gestione di una sequenza di intestazione della richiesta appositamente predisposta. Un utente malintenzionato remoto non autenticato può sfruttarlo per arrestare il servizio o forzare ap_find_token() a restituire un valore errato. (CVE-2017-7668)

- Esiste una vulnerabilità Denial of Service in httpd a causa di un errore di lettura fuori limite nel mod_mime che viene attivato durante la gestione di un'intestazione di risposta Content-Type appositamente predisposta. Un utente malintenzionato remoto non autenticato può sfruttarlo per divulgare informazioni riservate o causare una condizione di negazione del servizio. (CVE-2017-7679)

- Esiste una vulnerabilità di negazione del servizio in httpd a causa di un errore nell'inizializzazione o nella reimpostazione del segnaposto del valore nelle intestazioni [Proxy-]Authorization di tipo 'Digest' prima o tra le successive assegnazioni chiave=valore da parte di mod_auth_digest. Un utente malintenzionato remoto non autenticato può sfruttarlo fornendo una chiave iniziale senza '='

incarico, per divulgare informazioni sensibili o causare una condizione di negazione del servizio. (CVE-2017-9788)

Si noti che Nessus non ha testato questi problemi, ma ha invece fatto affidamento solo sul numero di versione dell'applicazione segnalato dall'utente.

Guarda anche

https://archive.apache.org/dist/httpd/CHANGES_2.2.34

https://httpd.apache.org/security/vulnerabilities_22.html

Soluzione

Aggiorna ad Apache versione 2.2.34 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

6.7

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

Riferimenti

OFFERTA	99134
OFFERTA	99135
OFFERTA	99137
OFFERTA	99170
OFFERTA	99569
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7668
CVE	CVE-2017-7679
CVE	CVE-2017-9788

Informazioni sul plug-in

Pubblicato: 18/07/2017, Modificato: 17/09/2018

Uscita del plug-in

tcp/80/www

```
Fonte                     : Server: Apache/2.2.8 (Ubuntu) DAV/2
Versione installata: 2.2.8 Versione
fissa                     : 2.2.34
```

158900 - Apache 2.4.x < 2.4.53 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.53. Pertanto, è affetto da molteplici vulnerabilità come indicato nell'advisory 2.4.53.

- mod_lua Uso di un valore non inizializzato di in r:parsebody: un corpo della richiesta accuratamente predisposto può causare una lettura in un'area di memoria casuale che potrebbe causare l'arresto anomalo del processo. Questo problema interessa Apache HTTP Server 2.4.52 e versioni precedenti. Ringraziamenti: Chamal De Silva (CVE-2022-22719)

- Contrabbando di richieste HTTP: Apache HTTP Server 2.4.52 e versioni precedenti non riescono a chiudere la connessione in entrata quando si verificano errori scartando il corpo della richiesta, esponendo il server a HTTP Request Smuggling Ringraziamenti: James Kettle <james.kettle portswigger.net> (CVE-2022 -22720)

- Possibile overflow del buffer con LimitXMLRequestBody molto grande o illimitato nel core: se LimitXMLRequestBody è impostato per consentire corpi di richiesta superiori a 350 MB (predefinito a 1 M) su sistemi a 32 bit, si verifica un overflow di numeri interi che in seguito provoca scritture fuori limite. Questo problema interessa Apache HTTP Server 2.4.52 e versioni precedenti. Ringraziamenti: Collaborazione anonima con Trend Micro Zero Day Initiative (CVE-2022-22721)

- Lettura/scrittura oltre i limiti in mod_sed: la vulnerabilità di scrittura fuori limite in mod_sed di Apache HTTP Server consente a un utente malintenzionato di sovrascrivere la memoria dell'heap con i dati eventualmente forniti dall'attaccante. Questo problema interessa Apache HTTP Server 2.4 versione 2.4.52 e versioni precedenti. Ringraziamenti: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

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

http://www.apache.org/dist/httpd/Announcement2.4.html

https://httpd.apache.org/security/vulnerabilities_24.html

Soluzione

Aggiorna ad Apache versione 2.4.53 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

7.4

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XRIF	IAVA:2022-A-0124-S

Informazioni sul plug-in

Pubblicato: 14/03/2022, Modificato: 15/06/2022

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.53
```

161948 - Apache 2.4.x < 2.4.54 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.54. Pertanto, è affetto da molteplici vulnerabilità come indicato nell'advisory 2.4.54.

- Possibile contrabbando di richieste in mod_proxy_ajp: la vulnerabilità dell'interpretazione incoerente delle richieste HTTP ("contrabbando di richieste HTTP") in mod_proxy_ajp di Apache HTTP Server consente a un utente malintenzionato di contrabbandare richieste al server A JP a cui inoltra le richieste. Questo problema riguarda Apache HTTP Server Apache HTTP Server 2.4 versione 2.4.53 e versioni precedenti. Ringraziamenti: Ricter Z @ 360 Noah Lab (CVE-2022-26377)

- Lettura oltre i limiti in mod_isapi: Apache HTTP Server 2.4.53 e versioni precedenti su Windows potrebbero leggere oltre i limiti se configurato per elaborare le richieste con il modulo mod_isapi. Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Ronald Crane (Zippenhop LLC) per aver segnalato questo problema (CVE-2022-28330)

- Leggi oltre i limiti tramite ap_rwrite(): la funzione ap_rwrite() in Apache HTTP Server 2.4.53 e versioni precedenti potrebbe leggere la memoria non intenzionale se un utente malintenzionato può far sì che il server rifletta un input molto grande utilizzando ap_rwrite() o ap_rputs(), come con la funzione mod_luas r:puts(). Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Ronald Crane (Zippenhop LLC) per aver segnalato questo problema (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 e versioni precedenti potrebbero arrestarsi in modo anomalo o divulgare informazioni a causa di una lettura oltre i limiti in ap_strcmp_match() quando viene fornito con un buffer di input estremamente grande. Sebbene nessun codice distribuito con il server possa essere forzato in tale chiamata, i moduli di terze parti o gli script lua che utilizzano ap_strcmp_match() potrebbero ipoteticamente essere influenzati. Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Ronald Crane (Zippenhop LLC) per aver segnalato questo problema (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: in Apache HTTP Server 2.4.53 e versioni precedenti, una richiesta dannosa a uno script lua che chiama r:parsebody(0) può causare un denial of service a causa dell'assenza di un limite predefinito sulla possibile dimensione di input . Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Ronald Crane (Zippenhop LLC) per aver segnalato questo problema (CVE-2022-29404)

- Denial of Service mod_sed: se Apache HTTP Server 2.4.53 è configurato per eseguire trasformazioni con mod_sed in contesti in cui l'input a mod_sed può essere molto grande, mod_sed può eseguire allocazioni di memoria eccessivamente grandi e attivare un'interruzione. Ringraziamenti: questo problema è stato rilevato da Brian Moussalli del team JFrog Security Research (CVE-2022-30522)

- Divulgazione di informazioni in mod_lua con websocket: Apache HTTP Server 2.4.53 e versioni precedenti possono restituire lunghezze alle applicazioni che chiamano r:wsread() che puntano oltre la fine dello spazio di archiviazione allocato per il buffer.

Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Ronald Crane (Zippenhop LLC) per aver segnalato questo problema (CVE-2022-30556)

- X-Forwarded-For eliminato dal meccanismo hop-by-hop in mod_proxy: Apache HTTP Server 2.4.53 e versioni precedenti potrebbero non inviare le intestazioni X-Forwarded-* al server di origine in base all'intestazione della connessione lato client hop-by-hop meccanismo. Questo può essere utilizzato per ignorare l'autenticazione basata su IP sul server/applicazione di origine.

Ringraziamenti: il progetto Apache HTTP Server desidera ringraziare Gaetan Ferry (Synacktiv) per aver segnalato questo problema (CVE-2022-31813)

Si noti che Nessus non ha testato questi problemi, ma ha invece fatto affidamento solo sul numero di versione dell'applicazione segnalato dall'utente.

Guarda anche

https://httpd.apache.org/security/vulnerabilities_24.html

Soluzione

Aggiorna ad Apache versione 2.4.54 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

7.4

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2022-26377
CVE	CVE-2022-28330
CVE	CVE-2022-28614
CVE	CVE-2022-28615
CVE	CVE-2022-29404
CVE	CVE-2022-30522
CVE	CVE-2022-30556

CVE	CVE-2022-31813
XRIF	IAVA:2022-A-0230-S

Informazioni sul plug-in

Pubblicato: 2022/06/08, Modificato: 2023/01/19

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.54
```

170113 - Apache 2.4.x < 2.4.55 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.55. Pertanto, è affetto da molteplici vulnerabilità come indicato nell'advisory 2.4.55.

- Un'intestazione della richiesta If: attentamente predisposta può causare una lettura o scrittura della memoria di un singolo byte zero, in una posizione di memoria del pool (heap) oltre il valore dell'intestazione inviato. Ciò potrebbe causare l'arresto anomalo del processo. Questo problema interessa Apache HTTP Server 2.4.54 e versioni precedenti. (CVE-2006-20001)

- La vulnerabilità dell'interpretazione incoerente delle richieste HTTP ("HTTP Request Smuggling") in mod_proxy_ajp di Apache HTTP Server consente a un utente malintenzionato di contrabbandare richieste al server A JP a cui inoltra le richieste. Questo problema riguarda Apache HTTP Server Apache HTTP Server 2.4 versione 2.4.54 e versioni precedenti.

(CVE-2022-36760)

- Prima di Apache HTTP Server 2.4.55, un back-end dannoso può causare il troncamento anticipato delle intestazioni della risposta, con conseguente incorporazione di alcune intestazioni nel corpo della risposta. Se le intestazioni successive hanno uno scopo di sicurezza, non verranno interpretate dal client. (CVE-2022-37436)

Si noti che Nessus non ha testato questi problemi, ma ha invece fatto affidamento solo sul numero di versione dell'applicazione segnalato dall'utente.

Soluzione

Aggiorna ad Apache versione 2.4.55 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

7.3

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2006-20001
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XRIF	IAVA:2023-A-0047-S

Informazioni sul plug-in

Pubblicato: 18/01/2023, Modificato: 10/03/2023

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.55
```

172186 - Apache 2.4.x < 2.4.56 Vulnerabilità multiple

Sinossi

Il server web remoto è affetto da molteplici vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.56. Pertanto, è affetto da molteplici vulnerabilità come indicato nell'advisory 2.4.56.

- Suddivisione della richiesta HTTP con mod_rewrite e mod_proxy: alcune configurazioni mod_proxy su Apache HTTP Server versioni da 2.4.0 a 2.4.55 consentono un attacco di contrabbando di richieste HTTP. Le configurazioni sono interessate quando mod_proxy è abilitato insieme a qualche forma di RewriteRule o ProxyPassMatch in cui un modello non specifico corrisponde a una parte della richiesta-target (URL) fornita dall'utente
dati e viene quindi reinserito nella destinazione della richiesta proxy utilizzando la sostituzione delle variabili. Ad esempio, qualcosa come: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http:// example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http:// example.com:8080/ La suddivisione/il contrabbando delle richieste potrebbe comportare l'elusione dei controlli di accesso nel server proxy, l'inoltro di URL non desiderati ai server di origine esistenti e avvelenamento della cache. Ringraziamenti: cercatore: Lars Krapf di Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi Suddivisione della risposta HTTP: Vulnerabilità del contrabbando di risposta HTTP in Apache HTTP Server tramite mod_proxy_uwsgi. Questo problema interessa Apache HTTP Server: dalla 2.4.30 alla 2.4.55.

I caratteri speciali nell'intestazione della risposta di origine possono troncare/dividere la risposta inoltrata al client.

Ringraziamenti: cercatore: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Si noti che Nessus non ha testato questi problemi, ma ha invece fatto affidamento solo sul numero di versione dell'applicazione segnalato dall'utente.

Soluzione

Aggiorna ad Apache versione 2.4.56 o successiva.

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 temporale CVSS v3.0

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

Punteggio VPR

9.4

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

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XRIF	IAVA:2023-A-0124

Informazioni sul plug-in

Pubblicato: 07/03/2023, Modificato: 15/03/2023

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.56
```

153583 - Apache < 2.4.49 Vulnerabilità multiple

Sinossi

Il server Web remoto è interessato da una vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.49. È, quindi, affetto da una vulnerabilità a cui si fa riferimento nel log delle modifiche 2.4.49.

- Un percorso uri di richiesta predisposto può far sì che mod_proxy inoltri la richiesta a un server di origine scelto dall'utente remoto. (CVE-2021-40438)

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://downloads.apache.org/httpd/CHANGES_2.4 https://
httpd.apache.org/security/vulnerabilities_24.html

Soluzione

Aggiorna ad Apache versione 2.4.49 o successiva.

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

8.1

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

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2021-40438
XRIF	IAVA:2021-A-0440-S
XRIF	CISA-NOTA-SFRUTTATA:2021/12/15

Informazioni sul plug-in

Pubblicato: 23/09/2021, Modificato: 25/04/2023

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.49
```

153584 - Apache < 2.4.49 Vulnerabilità multiple

Sinossi

Il server Web remoto è interessato da una vulnerabilità.

Descrizione

La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.49. È, quindi, affetto da molteplici vulnerabilità come indicato nel log delle modifiche 2.4.49.

- ap_escape_quotes() può scrivere oltre la fine di un buffer quando viene fornito un input dannoso. Nessun modulo incluso trasmette dati non attendibili a queste funzioni, ma i moduli di terze parti/esterni possono farlo. (CVE-2021-39275)

- Le richieste malformate possono causare la dereferenziazione di un puntatore NULL da parte del server. (CVE-2021-34798)

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://downloads.apache.org/httpd/CHANGES_2.4 https://

httpd.apache.org/security/vulnerabilities_24.html

Soluzione

Aggiorna ad Apache versione 2.4.49 o successiva.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

7.4

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

STIG Gravità

IO

Riferimenti

CVE	CVE-2021-34798
CVE	CVE-2021-39275
XRIF	IAVA:2021-A-0440-S

Informazioni sul plug-in

Pubblicato: 23/09/2021, Modificato: 11/04/2022

Uscita del plug-in

tcp/80/www

```
URL                     : http://192.168.50.101/
Versione installata: 2.2.8 Versione
fissa                   : 2.4.49
```

70728 - Esecuzione di codice remoto Apache PHP-CGI

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 un difetto che potrebbe consentire a un utente malintenzionato remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Questo potrebbe essere abusato per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

Soluzione

Aggiorna a PHP 5.3.13 / 5.4.3 o successivo.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio VPR

8.9

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

Riferimenti

OFFERTA	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XRIF	CERT:520827

XRIF	EDB-ID:29290
XRIF	EDB-ID:29316
XRIF	CISA-NOTA-SFRUTTATA:2022/04/15

Sfruttabile con

CANVAS (vero) Core Impact (vero) Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 2013/11/01, Modificato: 2023/04/25

Uscita del plug-in

tcp/80/www

Nessus è stato in grado di verificare l'esistenza del problema utilizzando la seguente richiesta:

- taglio ---------- ----------
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D% 6F%6E+%2D%64+
%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73 %69%6E%2E%73%69%6D%75%6C%61%74%69%6F
%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C% 65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F
%70%65%6E%5F%62%61%73% 65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E %64%5F%
66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F% 72%63%65%5F
%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69% 72%65%63%74%5F%73%74%61%74%75%73%5F
%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: 192.168.50.101
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-
Language: en
Tipo di contenuto: application/x-www-form-urlencoded
Connessione: Keep-Alive
Contenuto-Lunghezza: 115
Agente utente: Mozilla/4.0 (compatibile; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache

Accetta: immagine/gif, immagine/x-xbitmap, immagine/jpeg, immagine/pjpeg, immagine/png, */*
<?php echo "Tipo di contenuto:testo/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1685625007';
  sistema('id'); morire; ?>
- taglio ---------- ----------

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

Sinossi

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

Descrizione

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

Guarda anche

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

http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u ?9dab109f
http://www.nessus.org/u?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)

Punteggio temporale CVSS v3.0

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

Punteggio VPR

9.0

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

Riferimenti

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

Informazioni sul plug-in

Pubblicato: 24/03/2020, Modificato: 31/05/2023

Uscita del plug-in

tcp/8009/ajp13

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

```
0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F 61 73 64 66 2F   . . . . HTTP/1.1.../asdf/
0x0010:  78 78 78 78 78 2E 6A 73 70 00 00 09 6C 6F 63 61 6C 68 6F 7 3 74   xxxxx.jsp..
0x0020:  00 FF FF 00 09 6C 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0   . localhost.....l
0x0030:  06 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 63 63 65 70   ocalhost..P.....
0x0040:  74 2D 4C 61 6E 67 75 61 67 65 00 00 0E 65 6E 2D 55 53 2C 65 6E   . . mantenere in vita...A
0x0050:  3B 71 3D 30 2E 35 00 A0 08 00 01 30 00 00 0F 41 63 63 65 70 74   ccept-Lingua..
0x0060:  2D 45 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 64 65 66   . en-US,en;q=0.5.
0x0070:  6C 61 74 65 2C 20 73 64 63 68 00 00 0D 43 61 63 68 65 2D 43 6F   . . . . 0...Accept-E
0x0080:  6E 74 72 6F 6C 00 00 09 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00   ncoding...gzip,
0x0090:  07 4D 6F 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D 49 6E   sgonfiare, sdch...
0x00A0:  73 65 63 75 72 65 2D 52 65 71 75 65 73 74 73 00 00 01 31 00 A0   Controllo cache...
0x00B0:  01 00 09 74 65 78 74 2F 68 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61   max-età=0.....Lu
0x00C0:  6C 68 6F 73 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C 65   zilla...Aggiorna-
0x00D0:  74 2E 69 6E 63 6C 75 64 65 2E 72 65 7175 65 73 74 5F 75 72 69 00   Richiesta insicura
0x00E0:  00 01 31 00 0A 00 1F 6A 61 76 61 78 2E 73 65 72 76 6C 65 74 2E   s...1.....testo/h
0x00F0:  69 6E 63 6C 75 64 65 2E 70 61 7 4 68 5F 69 6E 66 6F 00 00 0F 57   tml.....localhos
0x0100:  45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C 00 0A 00 22 6A 61 76   t...!javax.servl
0x0110:  61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C 75 64 65 2 E73 65   et.include.reque
0x0120:  72 76 6C 65 74 5F 70 61 74 68 00 00 00 00 FF                      st_uri...1....ja
0x0130:                                                                    vax.servlet.incl
0x0140:                                                                    ude.path_info...
0x0150:                                                                    WEB-INF/web.xml.
0x0160:                                                                    . . "javax.servlet
0x0170:                                                                    . include.servlet
0x0180:                                                                    _sentiero.....
```

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

171356 - Apache httpd SEoL (2.1.x <= x <= 2.2.x)

Sinossi

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

Descrizione

Secondo la sua versione, Apache httpd è compreso tra 2.1.x e 2.2.x. Pertanto, non è più gestito dal suo fornitore o fornitore.

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

Guarda anche

https://archive.apache.org/dist/httpd/Announcement2.2.txt

Soluzione

Aggiorna a una versione di Apache httpd attualmente supportata.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

Pubblicato: 10/02/2023, Modificato: 29/03/2023

Uscita del plug-in

tcp/80/www

```
URL                                                 :  http://192.168.50.101/
Versione installata                                 :  2.2.8
Sicurezza Fine vita                                 : 11 luglio 2017
Tempo dalla fine del ciclo di vita della sicurezza (stimato): 5 anni,      10 mesi, 26 giorni | 2151 giorni totali
```

51988 - Rilevamento Backdoor Bind Shell

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

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

Soluzione

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

Fattore di rischio

Critico

Punteggio base CVSS v3.0

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

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

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

Uscita del plug-in

tcp/1524/wild_shell

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


Ciò ha prodotto il seguente output troncato (limitato a 10 righe):
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - taglio ---------- ---------- root@metasploitable :/#
uid=0(root) gid=0(root) groups=0(root) root@metasploitable :/#


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

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 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/5432/postgresql

15890 - Idra: VNC

Sinossi

Potrebbe essere possibile determinare le password VNC tramite la forza bruta.

Descrizione

Questo plugin esegue Hydra per trovare le password VNC con la forza bruta.

Per utilizzare questo plug-in, inserisci il "File di accesso" e il "File delle password" nel

blocco delle impostazioni avanzate "Hydra (opzioni wrapper NASL)".

Soluzione

Modificare le password per gli account interessati.

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: 2004/12/01, Modificato: 2023/05/01

Uscita del plug-in

tcp/5900/vnc

Hydra ha scoperto le seguenti password VNC:

parola d'ordine

86072 - Rilevamento versione non supportata di ISC BIND

Sinossi

L'host remoto esegue una versione non supportata di ISC BIND.

Descrizione

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul server dei nomi remoto è 9.8.x o precedente. Pertanto, 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 di ISC BIND attualmente supportata.

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)

Riferimenti

XRIF	IAVA:0001-A-0541

Informazioni sul plug-in

Pubblicato: 22/09/2015, Modificato: 16/02/2021

Uscita del plug-in

udp/53/dns

```
Versione installata: 9.4.2 Versione
fissa                        : 9.11, 9.16, 9.17 o superiore
URL di fine supporto: https://www.isc.org/downloads/
```