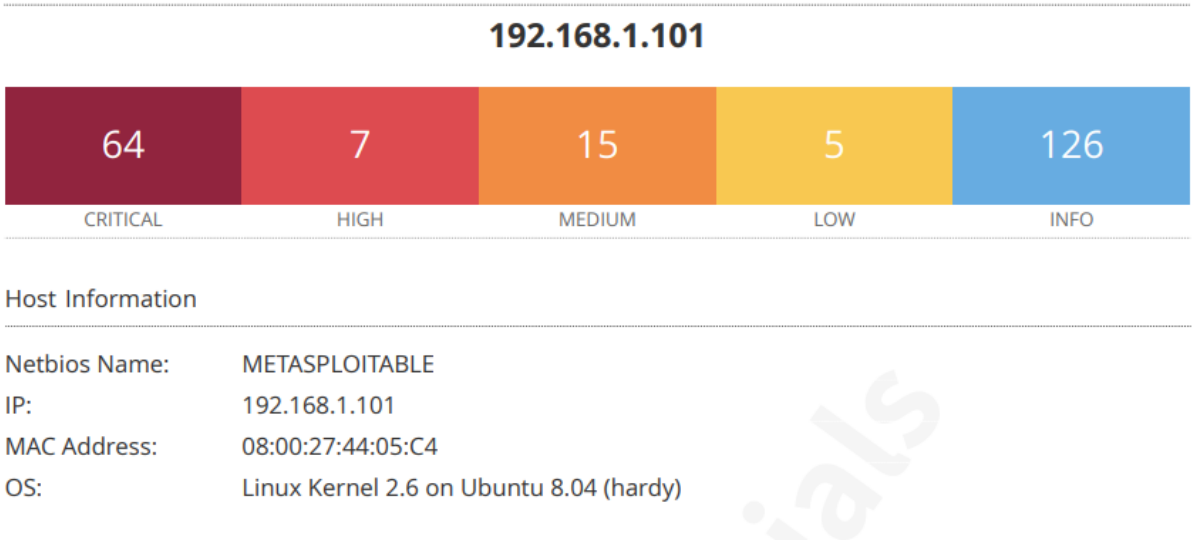
Report W12D1 – Scansione vulnerabilità Metasploitable (192.168.1.101) **Peppoli**

Per la scansione delle vulnerabilità di Metasploitable utilizzeremo Nessus, uno dei software più rinomati per la scansione e la valutazione della sicurezza informatica. È un potente strumento progettato per identificare vulnerabilità nei sistemi informatici, rilevare configurazioni non sicure e individuare potenziali minacce alla sicurezza. Nessus utilizza una vasta gamma di test e tecniche per esaminare reti, server, dispositivi e applicazioni alla ricerca di punti deboli che potrebbero essere sfruttati da attaccanti informatici. Il software fornisce report dettagliati e raccomandazioni per aiutare gli amministratori di sistema e i professionisti della sicurezza a mitigare i rischi e rafforzare la sicurezza delle infrastrutture IT.

Elenco delle vulnerabilità trovate:



Come si può notare abbiamo trovato:
Critiche: Queste sono le vulnerabilità più serie e potenzialmente dannose per un sistema. Possono consentire agli attaccanti di ottenere accesso completo al sistema o di eseguire codice dannoso senza autenticazione.

Alte: Le vulnerabilità considerate di gravità alta possono ancora costituire una minaccia significativa per la sicurezza dei sistemi. Possono consentire l'accesso non autorizzato o l'esecuzione di azioni dannose, anche se potrebbero richiedere condizioni specifiche per essere sfruttate.

Medie: Le vulnerabilità di gravità media rappresentano un rischio meno critico rispetto alle precedenti, ma possono comunque essere sfruttate dagli aggressori per compromettere la sicurezza dei sistemi.

Basse: Queste vulnerabilità sono considerate meno critiche e possono rappresentare un rischio limitato per la sicurezza. Tuttavia, è comunque consigliabile correggerle per mantenere un livello ottimale di sicurezza.

Informative (Info): Questo tipo di vulnerabilità fornisce informazioni aggiuntive sul sistema, come configurazioni non ottimali o informazioni sul software utilizzato. Anche se non rappresentano un rischio diretto per la sicurezza, possono essere utili per migliorare la configurazione e la gestione del sistema.

Nessus identifica queste vulnerabilità attraverso una serie di test e controlli che esaminano le configurazioni di sistema, le versioni del software, le patch applicate e altri fattori che potrebbero influenzare la sicurezza complessiva del sistema.

Valutiamo una vulnerabilità per tipo:

134862 - Inserimento richiesta connettore Apache Tomcat AJP (Ghostcat)

Vulnerabilità Critica

Riepilogo: È presente un connettore AJP vulnerabile in ascolto sull'host remoto.

Descrizione: È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni 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 in modalità remota (RCE).

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

Fattore di rischio: Alto

10205 - Rilevamento del servizio rlogin

Vulnerabilità Alta

Riepilogo: Il servizio rlogin è in esecuzione sull' host remoto.

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

Soluzione: Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.

Fattore di rischio: Alto

11213 - Metodi HTTP TRACE/TRACK consentiti

Vulnerabilità media

Riepilogo: 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 del server Web.

Soluzione: Disabilita questi metodi HTTP. Fare riferimento all'output del plugin per ulteriori informazioni.

Fattore di rischio: medio

10407 - Rilevamento server X

Vulnerabilità bassa

Riepilogo: Un server X11 è in ascolto sull'host remoto.

Descrizione: L'host remoto esegue un server X11, un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto. Poiché il traffico X11 non viene cifrato, è possibile che un utente malintenzionato possa intercettare la connessione.

Soluzione: Limita l'accesso a questa porta. Se la funzionalità client/server di X11 non viene utilizzata, disabilita completamente il supporto TCP in X11 (- nolisten tcp).

Fattore di rischio: basso

39519 - Rilevamento patch di sicurezza con backport (FTP)

Vulnerabilità info

Riepilogo: Le patch di sicurezza sono sottoposte a backport.

Descrizione: Le patch di sicurezza potrebbero essere state "backported" sul server FTP remoto senza modificarne il numero di versione. I controlli basati su banner sono stati disabilitati per evitare falsi positivi. Tieni presente che questo test è solo informativo e non denota alcun problema di sicurezza.

Soluzione: n/a

Fattore di rischio: nessuno

In seguito, riportate le stesse vulnerabilità, ma descritte in maniera più dettagliata.

134862 - Inserimento richiesta connettore Apache Tomcat AJP (Ghostcat)

Sinossi

È presente un connettore AJP vulnerabile in ascolto sull'host remoto.

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni 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 in modalità remota (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 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

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 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
XREF	CISA-NOTO-SFRUTTATO:2022/03/17
XREF	ID CEA: CEA-2020-0021

Informazioni sul plug-in

Pubblicato: 24/03/2020, Modificato: 25/09/2023

Uscita del plugin

tcp/8009/ajp13

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

```
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F 0x0010: 61 73 64 66 2F 78 78 78 78
78 2E 6A 73 70 00 00
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C 0x0030: 6F 63 61 6C 68 6F 73 74 00
00 50 00 00 09 A0 06
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 0x0050: 63 63 65 70 74 2D 4C 61 6E
67 75 61 67 65 00 00 0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00

0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 0x0080: 6E 63 6F 64 69 6E 67 00 00
13 67 7A 69 70 2C 20
65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09 Controllo cache...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F età massima=0.....Mo
0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D 0x00D0: 49 6E 73 65 63 75 72 65 2D
52 65 71 75 65 73 74
0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68 0x00F0: 74 6D 6C 00 A0 0B 00 09 6C
6F 63 61 6C 68 6F 73 0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C

0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65 0x0120: 73 74 5F 75 72 69 00 00 01
31 00 0A 00 1F 6A 61
0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C vax.servlet.incl
0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10 0x0150: 2F 57 45 42 2D 49 4E 46 2F
77 65 62 2E 78 6D 6C
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65 0x0170: 74 2E 69 6E 63 6C 75 64 65
2E 73 65 72 76 6C 65
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF
```

```
....HTTP/1.1.../
asdf/xxxxx.jsp..
.localhost.....l
ocalhost..P.....
..mantieniti in vita...A
ccept-Lingua..
.en-USA,en;q=0,5.
....0...Accetta-E
ncoding...gzip, 0x0090: 64


zilla...Richiesta di
aggiornamento non sicura
s...1.....testo/h
tml.....localhos
t...!javax.servl
e.includi.richiesta
st_uri...1....ja

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

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

10205 - Rilevamento del servizio rlogin

Sinossi

Il servizio rlogin è in esecuzione sull'host remoto.

Descrizione

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

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

Soluzione

Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.

Fattore di rischio

Alto

Punteggio base CVSS v2.0

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

Riferimenti

CVE	CVE-1999-0651

Sfruttabile con

Metasploit (vero)

Informazioni sul plug-in

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

Uscita del plugin

tcp/513/rlogin

11213 - Metodi HTTP TRACE/TRACK consentiti

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 del server Web.

Guarda anche

http://www.nessus.org/u?e979b5cb http://

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

download.oracle.com/sunalerts/1000718.1.html

Soluzione

Disabilita questi metodi HTTP. Fare riferimento all'output del plugin per ulteriori informazioni.

Fattore di rischio

medio

Punteggio base CVSS v3.0

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

Punteggio temporale CVSS v3.0

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

Punteggio base CVSS v2.0

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

Punteggio temporale CVSS v2.0

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

Riferimenti

OFFERTA	9506
OFFERTA	9561
OFFERTA	11604
OFFERTA	33374

OFFERTA	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERTIFICATO:288308
XREF	CERTIFICATO:867593
XREF	CWE:16
XREF	CWE:200

Informazioni sul plug-in

Pubblicato: 23/01/2003, Modificato: 27/10/2023

Uscita del plugin

tcp/80/www

Per disabilitare questi metodi, aggiungi le seguenti righe per ciascun host virtuale nel file di configurazione:

```
RewriteEngine su RewriteCond
%{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

In alternativa, tieni presente che le versioni Apache 1.3.34, 2.0.55 e 2.2 supportano la disabilitazione del metodo TRACE
in modo nativo tramite la direttiva 'TraceEnable'.

Nessus ha inviato la seguente richiesta TRACE: \n\n------------------------------ snip
---------------------------------\nTRACE /Nessus891368769.html HTTP/1.1
Connessione: chiusa
Ospite: 192.168.1.101
Pragma: agente utente no-
cache: Mozilla/4.0 (compatibile; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accetta: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Lingua di accettazione: en Set di caratteri di accettazione:
iso-8859-1,*,utf-8

------------------------------ ritaglia ------------------ ----------\n\ne ho ricevuto la seguente risposta dal server remoto:\n\n---------------------- -------- taglia ----------
\nHTTP/1.1 200 OK

Data: martedì 27 febbraio 2024 18:14:45 GMT Server: Apache/
2.2.8 (Ubuntu) DAV/2 Keep-Alive: timeout=15, max=100
Connessione: Keep-Alive Codifica trasferimento: Chunked
Content-Type : messaggio/http

TRACE /Nessus891368769.html Connessione HTTP/1.1: Keep-Alive

Ospite: 192.168.1.101
Pragma: agente utente no-
cache: Mozilla/4.0 (compatibile; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accetta: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Lingua di accettazione: en Set di caratteri di accettazione:
iso-8859-1,*,utf-8

------------------------------ ritaglia ------------------ ----------\N

10407 - Rilevamento server X

Sinossi

Un server X11 è in ascolto sull'host remoto

Descrizione

L'host remoto esegue un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto.

Poiché il traffico X11 non viene cifrato, è possibile che un utente malintenzionato possa intercettare la connessione.

Soluzione

Limita l'accesso a questa porta. Se la funzionalità client/server di X11 non viene utilizzata, disabilita completamente il supporto TCP in X11 (- nolisten tcp).

Fattore di rischio

Basso

Punteggio base CVSS v2.0

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

Informazioni sul plug-in

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

Uscita del plugin

tcp/6000/x11

```
Versione X11: 11.0
```

39519 - Rilevamento patch di sicurezza con backport (FTP)

Sinossi

Le patch di sicurezza sono sottoposte a backport.

Descrizione

Le patch di sicurezza potrebbero essere state "backported" sul server FTP remoto senza modificarne il numero di versione.

I controlli basati su banner sono stati disabilitati per evitare falsi positivi.

Tieni presente che questo test è solo informativo e non denota alcun problema di sicurezza.

Guarda anche

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Soluzione

n / a

Fattore di rischio

Nessuno

Informazioni sul plug-in

Pubblicato: 25/06/2009, Modificato: 07/07/2015

Uscita del plugin

tcp/2121/ftp

Fornire le credenziali a Nessus per eseguire controlli locali.