

CSPT 0524

Vulnerabilità risolte:

1. Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVE-2020-1938)

Sono entrato nel file server.xml di tomcat5.5 e ho commentato la stringa riguardante la porta 8009 come segue, disabilitando il connettore:

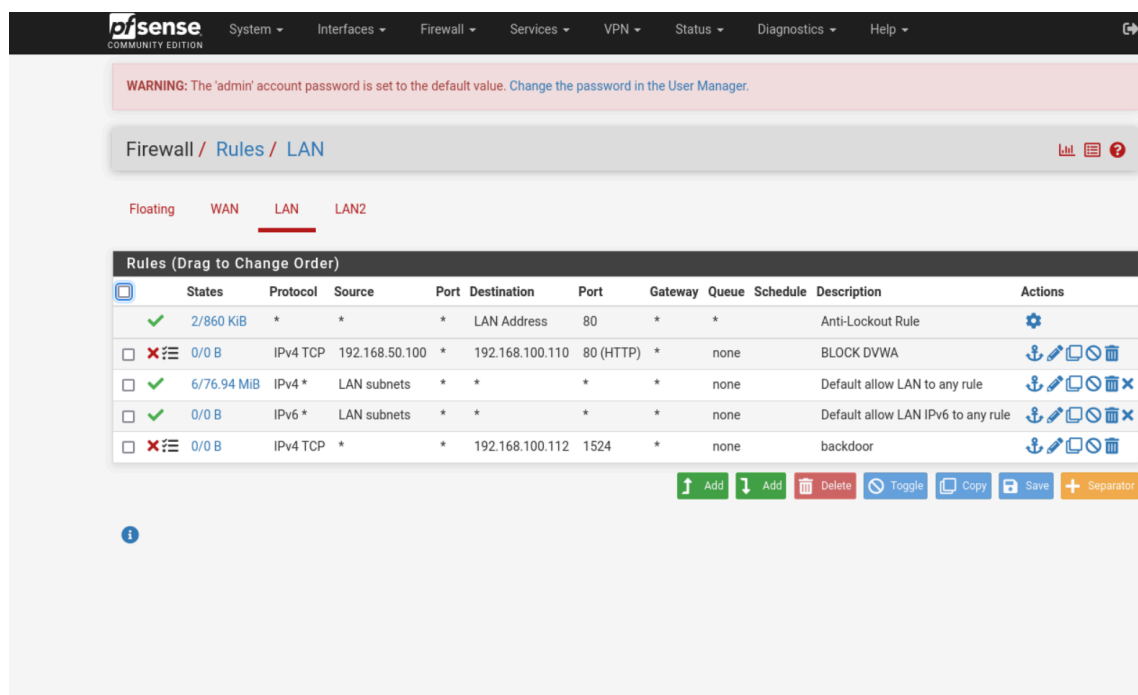
```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml      Modified
-->
    clientAuth="false" sslProtocol="TLS" />
-->
<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009"
    enableLookups="false" redirectPort="8443" protocol="AJP/1.3" /> $
```

Poi, ho restartato Tomcat utilizzando il comando "init.d".

2. Bind Shell Backdoor Detection (porta 1524)

- Rilevata nel primo report (09/02/2025) come una backdoor che permetteva l'accesso remoto non autenticato.
- Nel secondo report (10/02/2025), questa vulnerabilità non compare più, il che indica che la backdoor è stata rimossa.

Ho inserito una regola firewall su pfsense come da screen per bloccare la porta 1524:



3.UnrealIRCd Backdoor Detection (porta 6667)

- Presente nella prima scansione, indicava la presenza di una versione compromessa di UnrealIRCd.
- Non più presente nel secondo report.

Ho rimosso unrealircd, killando il processo ed eliminando tutti i file del sw.

```
g jdoc          ucf
gkeytool        ucfq
gkeytool-4.2    ucfr
gnative2ascii-4.2 ucs2any
gorbd           udevinfo
gorbd-4.2       udevtest
gpasswd         ul
gpg             unexpand
gpg-converter-from-106 unicode_start
gpgsplit        unicode_stop
gpgv            uniq
gpg-zip         unlink
gpic            unlzma
gprof           unzip
grep-excuses    unzipsfx
grepjar         updatedb
grmic-4.2       updatedb.mlocate
grmid           update-menus
grmid-4.2       update-pciids
grmiregistry    uptime
grmiregistry-4.2 uscan
groff           users
grog            uuidgen
grops           uupdate
groty           uxterm
```

```
ltrace          xtrapin
luit            xtrapinfo
lwp-download    xtrapout
lwp-mirror      xtrapproto
lwp-request     xtrapreset
lwp-rget        xtrapstats
lxterm          xvidtune
lzcat           xvinfo
lzma            Xvnc
lzma_alone      xwd
m4              x-window-manager
mailq           xwininfo
make            xwud
make-memtest86+-boot-floppy x-www-browser
make_method     xxd
man             yes
mandb           zdump
manpage-alert   zipgrep
manpath         zipinfo
mass-bug        zsoelim
mawk
msfadmin@metasploitable:~$ cd /usr/bin
msfadmin@metasploitable:~$ sudo rm -rf /etc/unrealircd
msfadmin@metasploitable:~$ find / -name "unrealircd*" 2>/dev/null
msfadmin@metasploitable:~$
```

4.VNC Server con password debole ("password") (porta 5900)

- La prima scansione segnalava l'accesso remoto tramite VNC con la password di default.
- Nella seconda scansione, questa vulnerabilità non compare più, perché ho cambiato la password VNC, killato il processo, restartato il servizio con il comando "init.d" facendolo partire sul display 0 con il comando:"vncserver :0"

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

VULNERABILITA' RISOLTE: 4