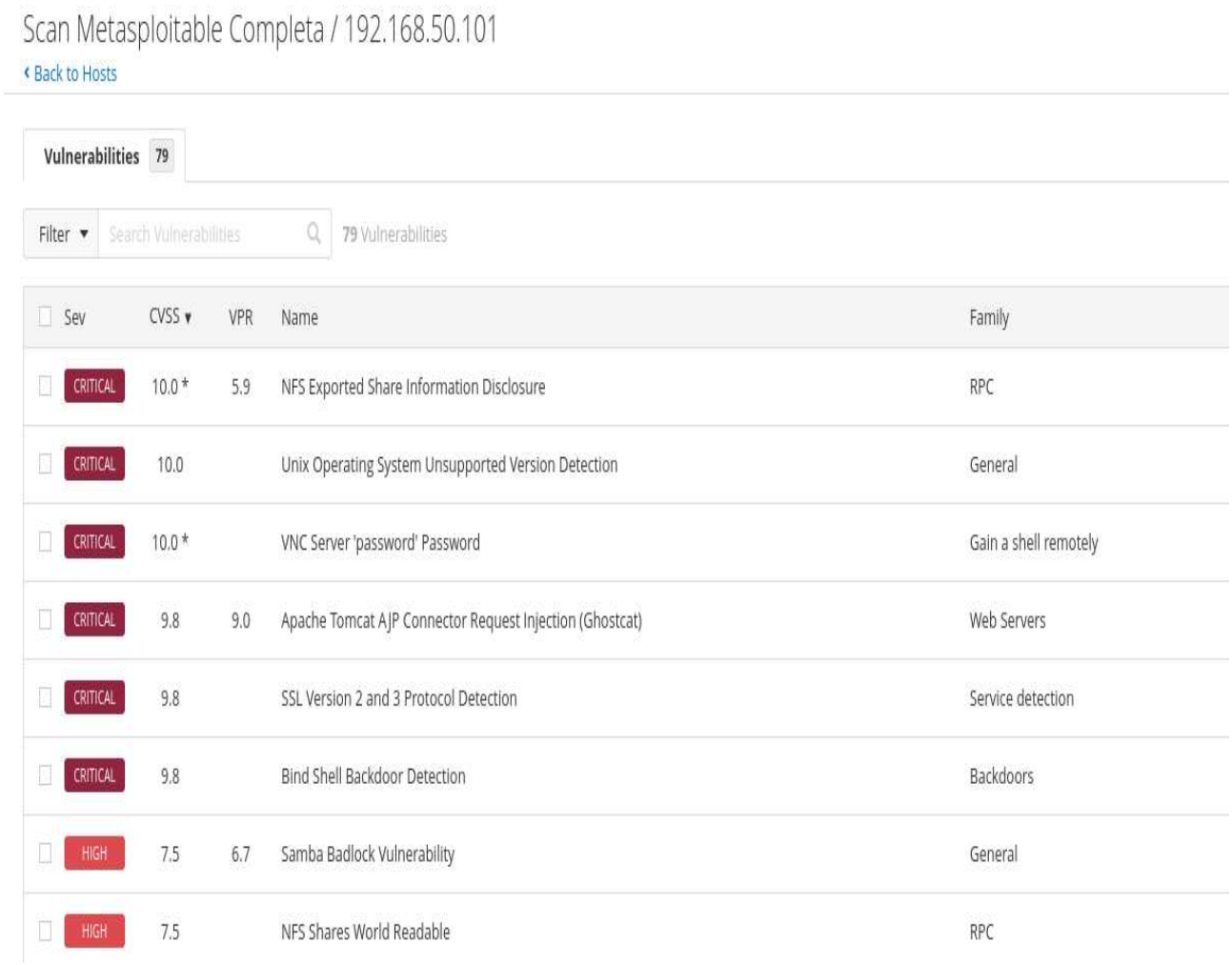
Effettuo un vulnerability assessment con **Nessus** sulla macchina Metasploitable.



Scan Metasploitable Completa / 192.168.50.101

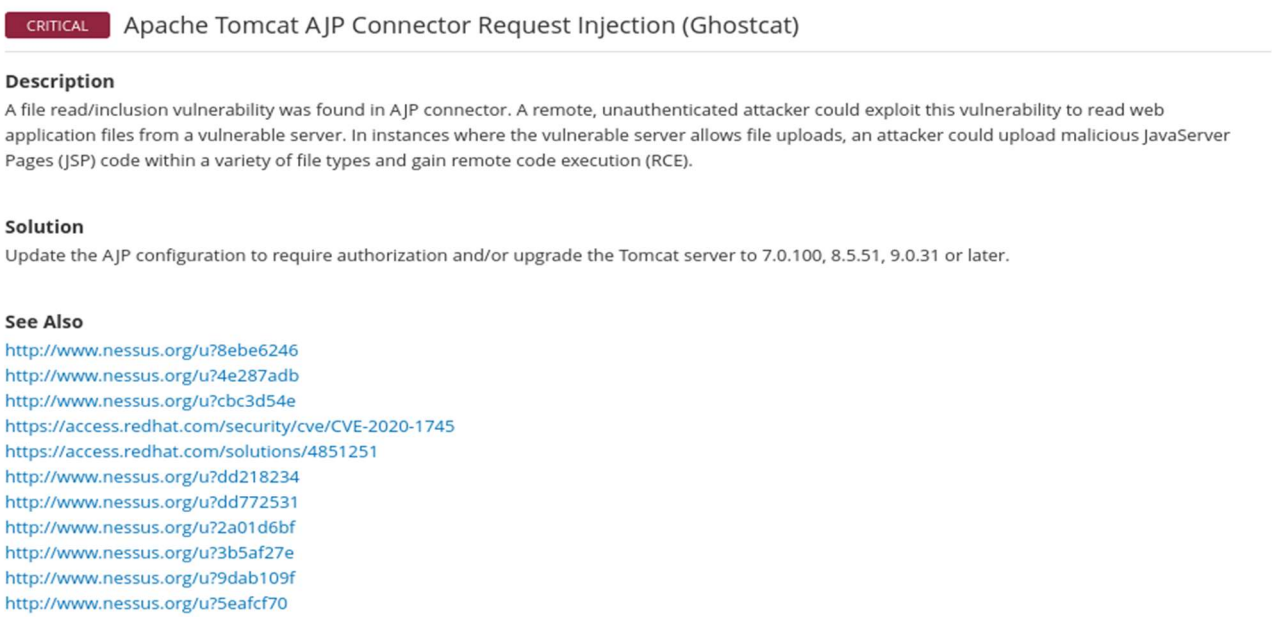
‹ Back to Hosts

Vulnerabilities 79

Filter ▾ Search Vulnerabilities 79 Vulnerabilities

Sev	CVSS ▾	VPR	Name	Family
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
HIGH	7.5	6.7	Samba Badlock Vulnerability	General
HIGH	7.5		NFS Shares World Readable	RPC

Aprendo una pagina specifica di una **vulnerabilità** troviamo una descrizione approfondita su di essa, la soluzione consigliata, link utili per l'approfondimento, l'output utilizzato dal tool per scovarla e dettagli su IP e porta.



CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

See Also

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

Output

```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0F 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
8009 / tcp / ajp13	192.168.50.101