



## Rete 192.168.50.0/24

---

Report generated by Tenable Nessus™

Tue, 24 Sep 2024 01:32:24 CEST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.50.1.....	4
• 192.168.50.103.....	6
• 192.168.50.104.....	11
• 192.168.50.106.....	13
• 192.168.50.107.....	14
• 192.168.50.108.....	15
• 192.168.50.109.....	19

Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.50.1



## Vulnerabilities

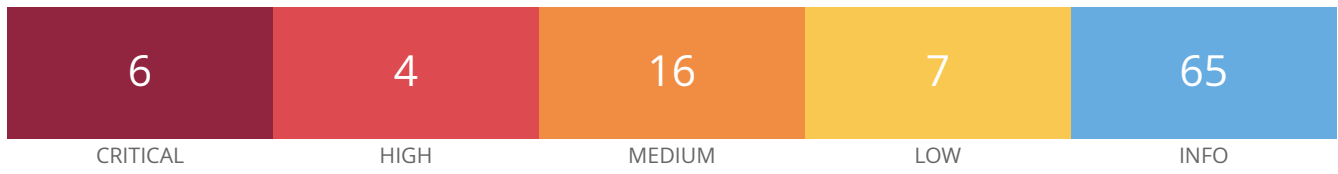
Total: 31

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.8	-	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">42822</a>	Strict Transport Security (STS) Detection
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">84821</a>	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	<a href="#">138330</a>	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">10386</a>	Web Server No 404 Error Code Check
INFO	N/A	-	-	<a href="#">106375</a>	nginx HTTP Server Detection
INFO	N/A	-	-	<a href="#">106952</a>	pfSense Detection
INFO	N/A	-	-	<a href="#">106198</a>	pfSense Web Interface Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.103



## Vulnerabilities

Total: 98

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.0967	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0967	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9725	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9524	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

MEDIUM	5.9	4.4	0.0054	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	0.0073	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	0.0114	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREEBIE)
LOW	3.7	3.6	0.5961	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	2.9	0.9736	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9749	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	<a href="#">10407</a>	X Server Detection
INFO	N/A	-	-	<a href="#">10223</a>	RPC portmapper Service Detection
INFO	N/A	-	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	-	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	-	<a href="#">10028</a>	DNS Server BIND version Directive Remote Version Detection

INFO	N/A	-	-	<a href="#">11002</a>	DNS Server Detection
INFO	N/A	-	-	<a href="#">35371</a>	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	<a href="#">132634</a>	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	<a href="#">10437</a>	NFS Share Export List
INFO	N/A	-	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">118224</a>	PostgreSQL STARTTLS Support
INFO	N/A	-	-	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	-	-	<a href="#">22227</a>	RMI Registry Detection
INFO	N/A	-	-	<a href="#">11111</a>	RPC Services Enumeration



INFO	N/A	-	-	<a href="#">53335</a>	RPC portmapper (TCP)
INFO	N/A	-	-	<a href="#">10263</a>	SMTP Server Detection
INFO	N/A	-	-	<a href="#">42088</a>	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	-	<a href="#">62563</a>	SSL Compression Methods Supported
INFO	N/A	-	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">17975</a>	Service Detection (GET request)
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided

INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	-	-	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	<a href="#">52703</a>	vsftpd Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.104



## Vulnerabilities

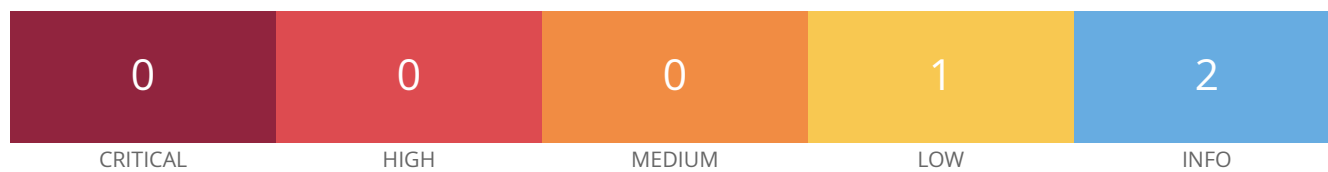
Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
HIGH	8.1	9.7	0.964	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	6.0	0.0192	90510	MS16-047: Security Update for SAM and LSAD Remote Protocol (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.3	-	-	57608	SMB Signing not required
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO	N/A	-	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">24786</a>	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.106



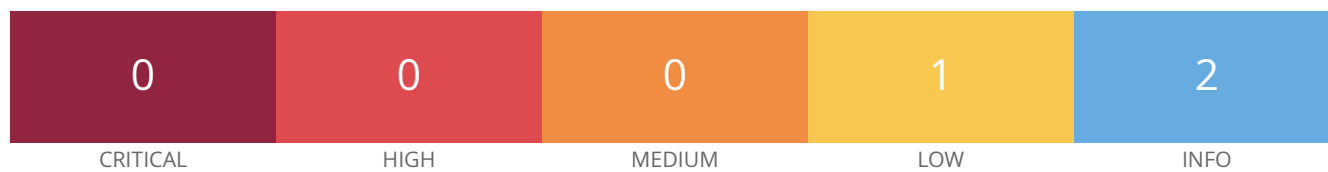
#### Vulnerabilities

Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.107



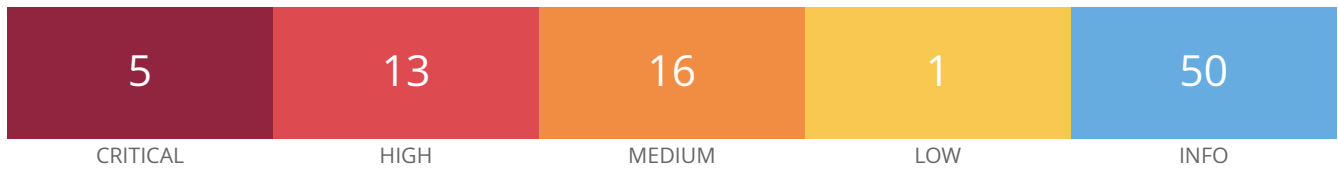
#### Vulnerabilities

Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.108



## Vulnerabilities

Total: 85

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	<a href="#">197843</a>	Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities
CRITICAL	9.8	6.7	0.0553	<a href="#">111066</a>	Apache Tomcat 7.0.0 < 7.0.89
CRITICAL	9.8	9.0	0.9728	<a href="#">134862</a>	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	7.4	0.9526	<a href="#">175373</a>	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJum
CRITICAL	10.0	-	-	<a href="#">171351</a>	Apache Tomcat SEoL (7.0.x)
HIGH	8.1	9.2	0.9744	<a href="#">103782</a>	Apache Tomcat 7.0.0 < 7.0.82
HIGH	8.1	8.4	0.9737	<a href="#">124064</a>	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities
HIGH	8.1	9.7	0.964	<a href="#">97833</a>	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.1	6.7	0.2633	<a href="#">100464</a>	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.5	6.7	0.0045	<a href="#">197838</a>	Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities
HIGH	7.5	4.4	0.017	<a href="#">197826</a>	Apache Tomcat 7.0.25 < 7.0.90
HIGH	7.5	3.6	0.148	<a href="#">138851</a>	Apache Tomcat 7.0.27 < 7.0.105
HIGH	7.5	3.6	0.0183	<a href="#">121121</a>	Apache Tomcat 7.0.28 < 7.0.88
HIGH	7.5	4.2	0.0111	<a href="#">35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.0	6.7	0.9141	<a href="#">136770</a>	Apache Tomcat 7.0.0 < 7.0.104
HIGH	7.0	6.7	0.0006	<a href="#">147163</a>	Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities

HIGH	7.5*	6.7	0.0004	<a href="#">10483</a>	PostgreSQL Default Unpassworded Account
MEDIUM	6.8	6.0	0.0192	<a href="#">90510</a>	MS16-047: Security Update for SAM and LSAD Remote Protocol (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	4.4	0.0028	<a href="#">106975</a>	Apache Tomcat 7.0.0 < 7.0.85 multiple vulnerabilities
MEDIUM	6.5	4.4	0.8755	<a href="#">10061</a>	Echo Service Detection
MEDIUM	6.5	4.4	0.8755	<a href="#">10198</a>	Quote of the Day (QOTD) Service Detection
MEDIUM	6.5	-	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	<a href="#">157288</a>	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.9	3.6	0.0023	<a href="#">148405</a>	Apache Tomcat 7.0.0 < 7.0.107
MEDIUM	5.9	4.4	0.0054	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	1.4	0.0032	<a href="#">106710</a>	Apache Tomcat 7.0.79 < 7.0.84
MEDIUM	5.3	-	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	4.3	2.2	0.7845	<a href="#">118035</a>	Apache Tomcat 7.0.23 < 7.0.91
MEDIUM	4.0	-	-	<a href="#">58453</a>	Terminal Services Doesn't Use Network Level Authentication (Only)
MEDIUM	5.0*	4.4	0.8755	<a href="#">10043</a>	Chargen UDP Service Remote DoS
LOW	2.1*	4.2	0.8808	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	-	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	-	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	-	<a href="#">10736</a>	DCE Services Enumeration
INFO	N/A	-	-	<a href="#">10052</a>	Daytime Service Detection
INFO	N/A	-	-	<a href="#">54615</a>	Device Type

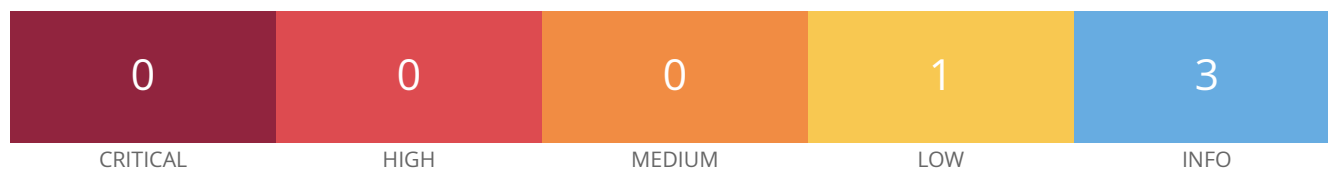


INFO	N/A	-	-	<a href="#">11367</a>	Discard Service Detection
INFO	N/A	-	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	-	<a href="#">84502</a>	HSTS Missing From HTTPS Server
INFO	N/A	-	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">174933</a>	Microsoft Message Queuing Detection
INFO	N/A	-	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	<a href="#">26917</a>	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">24786</a>	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	-	-	<a href="#">66173</a>	RDP Screenshot
INFO	N/A	-	-	<a href="#">10940</a>	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	-	<a href="#">10863</a>	SSL Certificate Information

INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.109



#### Vulnerabilities

Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	10287	Traceroute Information

\* indicates the v3.0 score was not available; the v2.0 score is shown