Rete 192.168.50.0/24

Report generated by Tenable Nessus™ Tue, 24 Sep 2024 01:32:24 CEST

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

Vulnerabilities by Host

192.168.50.1

0	0	3	1	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

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

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

192.168.50.103

6	4	16	7	65
CRITICAL	HIGH	MEDIUM	LOW	INFO

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 Obsolet and Weakened eNcryption)

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

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

INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
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	-	-	62563	SSL Compression Methods 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	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

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

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

192.168.50.104

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	2	1	21

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 Protoco (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 (remo check)

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

192.168.50.106

0	0	0	1	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

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

0	0	0	1	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

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

5	13	16	1	50
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 85

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	197843	Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities
CRITICAL	9.8	6.7	0.0553	111066	Apache Tomcat 7.0.0 < 7.0.89
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	7.4	0.9526	175373	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJum
CRITICAL	10.0	-	-	171351	Apache Tomcat SEoL (7.0.x)
HIGH	8.1	9.2	0.9744	103782	Apache Tomcat 7.0.0 < 7.0.82
HIGH	8.1	8.4	0.9737	124064	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities
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)
HIGH	8.1	6.7	0.2633	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.5	6.7	0.0045	197838	Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities
HIGH	7.5	4.4	0.017	197826	Apache Tomcat 7.0.25 < 7.0.90
HIGH	7.5	3.6	0.148	138851	Apache Tomcat 7.0.27 < 7.0.105
HIGH	7.5	3.6	0.0183	121121	Apache Tomcat 7.0.28 < 7.0.88
HIGH	7.5	4.2	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.0	6.7	0.9141	136770	Apache Tomcat 7.0.0 < 7.0.104
HIGH	7.0	6.7	0.0006	147163	Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities

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

INFO	N/A	-	-	11367	Discard Service Detection
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	174933	Microsoft Message Queuing Detection
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 (remo check)
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	66173	RDP Screenshot
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
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	-	-	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 (uncredentialed 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

0	0	0	1	3
CRITICAL	HIGH	MEDIUM	LOW	INFO

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