



## local

---

Report generated by Tenable Nessus™

Thu, 26 Jun 2025 12:03:01 IST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.1.1.....	4
• 192.168.1.3.....	6
• 192.168.1.5.....	7
• 192.168.1.9.....	11
• 192.168.1.10.....	12
• 192.168.1.11.....	13

Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.1.1



Vulnerabilities

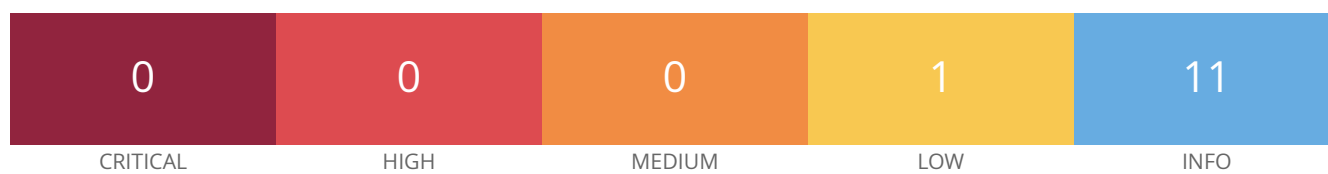
Total: 27

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	50686	IP Forwarding Enabled
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
LOW	3.3*	-	-	10663	DHCP Server Detection
LOW	2.1*	-	-	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	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
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	-	-	<a href="#">57041</a>	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="#">136318</a>	TLS Version 1.2 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

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

## 192.168.1.3



### Vulnerabilities

Total: 12

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information

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

192.168.1.5



Vulnerabilities

Total: 81

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.9	-	-	190856	Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Release
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	3.6	0.0004	193274	Suricata < 6.0.17 / 7.x < 7.0.4 DoS
HIGH	7.5	4.4	0.0004	214272	Suricata < 7.0.8 Multiple Vulnerabilities
HIGH	7.3	4.4	0.0012	206344	Suricata 6.x < 6.0.19 / 7.x < 7.0.5 Multiple Vulnerabilities
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	3.6	0.0005	214273	Suricata < 7.0.7 Multiple Vulnerabilities
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	189973	AnyDesk Installed (Linux)
INFO	N/A	-	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	-	106203	DHCP server Detection (Linux)
INFO	N/A	-	-	55472	Device Hostname
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	159488	Docker Installed (Linux)

INFO	N/A	-	-	<a href="#">93561</a>	Docker Service Detection
INFO	N/A	-	-	<a href="#">25203</a>	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	-	<a href="#">25202</a>	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	-	<a href="#">33276</a>	Enumerate MAC Addresses via SSH
INFO	N/A	-	-	<a href="#">170170</a>	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	-	<a href="#">179200</a>	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	-	<a href="#">168980</a>	Enumerate the PATH Variables
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="#">193599</a>	FFmpeg Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">168982</a>	Filepaths contain Dangerous characters (Linux)
INFO	N/A	-	-	<a href="#">84502</a>	HSTS Missing From HTTPS Server
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">171410</a>	IP Assignment Method Detection
INFO	N/A	-	-	<a href="#">200214</a>	Libndp Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">157358</a>	Linux Mounted Devices
INFO	N/A	-	-	<a href="#">193143</a>	Linux Time Zone Information
INFO	N/A	-	-	<a href="#">95928</a>	Linux User List Enumeration
INFO	N/A	-	-	<a href="#">195203</a>	Microsoft Azure Command-Line Interface (CLI) Installed (Linux)
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">64582</a>	Netstat Connection Information
INFO	N/A	-	-	<a href="#">14272</a>	Netstat Portscanner (SSH)
INFO	N/A	-	-	<a href="#">178771</a>	Node.js Installed (Linux / UNIX)
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH (Using New SSH Library)

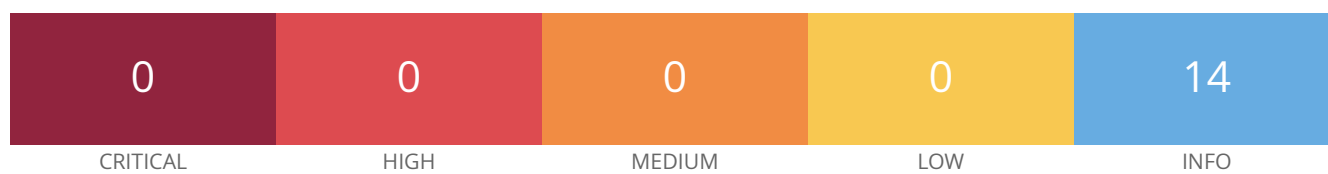


INFO	N/A	-	-	<a href="#">117887</a>	OS Security Patch Assessment Available
INFO	N/A	-	-	<a href="#">193272</a>	Open Information Security Foundation Suricata Installed (Linux)
INFO	N/A	-	-	<a href="#">168007</a>	OpenSSL Installed (Linux)
INFO	N/A	-	-	<a href="#">179139</a>	Package Manager Packages Report (nix)
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">130024</a>	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	-	<a href="#">119602</a>	Python Flask Installed (Linux)
INFO	N/A	-	-	<a href="#">212757</a>	RClone Installed (Linux)
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="#">202184</a>	Ruby Programming Language Installed (Linux)
INFO	N/A	-	-	<a href="#">133964</a>	SELinux Status Check
INFO	N/A	-	-	<a href="#">174788</a>	SQLite Local Detection (Linux)
INFO	N/A	-	-	<a href="#">56984</a>	SSL / TLS Versions Supported
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="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">94761</a>	SSL Root Certification Authority Certificate Information
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="#">22869</a>	Software Enumeration (SSH)
INFO	N/A	-	-	<a href="#">42822</a>	Strict Transport Security (STS) Detection
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="#">110095</a>	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	-	<a href="#">141118</a>	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	<a href="#">163326</a>	Tenable Nessus Installed (Linux)
INFO	N/A	-	-	<a href="#">56468</a>	Time of Last System Startup
INFO	N/A	-	-	<a href="#">192709</a>	Tukaani XZ Utils Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">83303</a>	Unix / Linux - Local Users Information : Passwords Never Expire
INFO	N/A	-	-	<a href="#">110483</a>	Unix / Linux Running Processes Information
INFO	N/A	-	-	<a href="#">152742</a>	Unix Software Discovery Commands Available
INFO	N/A	-	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	<a href="#">186361</a>	VMWare Tools or Open VM Tools Installed (Linux)
INFO	N/A	-	-	<a href="#">189731</a>	Vim Installed (Linux)
INFO	N/A	-	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">204828</a>	libexiv2 Installed (Linux / Unix)

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

192.168.1.9



## Vulnerabilities

Total: 14

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

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

192.168.1.10



## Vulnerabilities

Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information

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

192.168.1.11



## Vulnerabilities

Total: 34

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
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	5.3	-	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	-	42255	NFS Server Superfluous
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	19689	Embedded Web Server Detection
INFO	N/A	-	-	62351	Erlang Port Mapper Daemon Detection
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	11111	RPC Services Enumeration

INFO	N/A	-	-	<a href="#">53335</a>	RPC portmapper (TCP)
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="#">57041</a>	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="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	<a href="#">66717</a>	mDNS Detection (Local Network)

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