# Meta Nuova

Report generated by Nessus™

Wed, 06 Sep 2023 19:20:32 CEST

TABLE OF CONTENTS

## Vulnerabilities by Host

# Vulnerabilities by Host

# 192.168.1.1

| 10 | 1 | 3 | 0 | 41 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 55

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.0 | 9.2 | 156164 | Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution |
| CRITICAL | 10.0 | 10.0 | 156016 | Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| CRITICAL | 10.0 | 10.0 | 156257 | Apache Log4Shell RCE detection via callback correlation (Direct Check DNS) |
| CRITICAL | 10.0 | 10.0 | 156014 | Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156669 | Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC) |
| CRITICAL | 10.0 | 10.0 | 156258 | Apache Log4Shell RCE detection via callback correlation (Direct Check NTP) |
| CRITICAL | 10.0 | 10.0 | 156197 | Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS) |
| CRITICAL | 10.0 | 10.0 | 156232 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMB) |
| CRITICAL | 10.0 | 10.0 | 156375 | Apache Log4Shell RCE detection via callback correlation (Direct Check UPnP) |
| HIGH | 8.8 | 7.4 | 164017 | NodeJS System Information Library Command Injection (CVE-2021-21315) |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |

| | | | | |
|---|---|---|---|---|
| MEDIUM | 5.3 | - | 57608 | SMB Signing not required |
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| 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 | - | 84502 | HSTS Missing From HTTPS Server |
| INFO | N/A | - | 10107 | HTTP Server Type and Version |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| INFO | N/A | - | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | 11387 | L2TP Network Server Detection |
| INFO | N/A | - | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | - | 11011 | Microsoft Windows SMB Service Detection |
| INFO | N/A | - | 10395 | Microsoft Windows SMB Shares Enumeration |
| 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 | - | 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 | - | 66334 | Patch Report |
| INFO | N/A | - | 56984 | SSL / TLS Versions Supported |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 10863 | SSL Certificate Information |
| INFO | N/A | - | 159544 | SSL Certificate with no Common Name |
| 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 | - | 25240 | Samba Server Detection |
| INFO | N/A | - | 22964 | Service 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 | - | 10287 | Traceroute Information |
| INFO | N/A | - | 35711 | Universal Plug and Play (UPnP) Protocol Detection |
| INFO | N/A | - | 135860 | WMI Not Available |
| INFO | N/A | - | 10386 | Web Server No 404 Error Code Check |
| INFO | N/A | - | 35712 | Web Server UPnP Detection |
| INFO | N/A | - | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | - | 106375 | nginx HTTP Server Detection |

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

## 192.168.1.2

| 3 | 0 | 4 | 0 | 35 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 42

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| CRITICAL | 10.0 | 10.0 | 156197 | Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS) |
| CRITICAL | 10.0 | 10.0 | 156232 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMB) |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 5.3 | - | 57608 | SMB Signing not required |
| MEDIUM | 5.3 | - | 45411 | SSL Certificate with Wrong Hostname |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| 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 | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| INFO | N/A | - | 53513 | Link-Local Multicast Name Resolution (LLMNR) 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 (remote 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 | - | 43815 | NetBIOS Multiple IP Address Enumeration |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 10919 | Open Port Re-check |
| INFO | N/A | - | 66334 | Patch Report |
| 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 | - | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | - | 35297 | SSL Service Requests Client Certificate |
| INFO | N/A | - | 156899 | SSL/TLS Recommended Cipher Suites |
| INFO | N/A | - | 91263 | SSL/TLS Service Requires Client Certificate |
| INFO | N/A | - | 22964 | Service 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 | - | 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

# 192.168.1.23

| | | | | |
|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 11 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 13

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156375 | Apache Log4Shell RCE detection via callback correlation (Direct Check UPnP) |
| HIGH | 8.8 | 7.4 | 164017 | NodeJS System Information Library Command Injection (CVE-2021-21315) |
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 66334 | Patch Report |
| INFO | N/A | - | 10287 | Traceroute Information |
| INFO | N/A | - | 35711 | Universal Plug and Play (UPnP) Protocol Detection |
| INFO | N/A | - | 35712 | Web Server UPnP Detection |

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

# 192.168.1.90

| 23 | 7 | 18 | 7 | 72 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities

Total: 127

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.8 | 9.2 | 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 | 9.1 | 6.0 | 33447 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning |
| CRITICAL | 9.0 | 9.2 | 156164 | Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution |
| CRITICAL | 10.0 | 10.0 | 156016 | Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| CRITICAL | 10.0 | 10.0 | 156257 | Apache Log4Shell RCE detection via callback correlation (Direct Check DNS) |
| CRITICAL | 10.0 | 10.0 | 156115 | Apache Log4Shell RCE detection via callback correlation (Direct Check FTP) |
| CRITICAL | 10.0 | 10.0 | 156014 | Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156669 | Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC) |
| CRITICAL | 10.0 | 10.0 | 156197 | Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS) |
| CRITICAL | 10.0 | 10.0 | 156559 | Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND) |
| CRITICAL | 10.0 | 10.0 | 156232 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMB) |

|  |  |  |  |  |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156132 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP) |
| CRITICAL | 10.0 | 10.0 | 156166 | Apache Log4Shell RCE detection via callback correlation (Direct Check SSH) |
| CRITICAL | 10.0 | 10.0 | 156162 | Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet) |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 7.4 | 46882 | UnrealIRCd Backdoor Detection |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.8 | 7.4 | 164017 | NodeJS System Information Library Command Injection (CVE-2021-21315) |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 6.7 | 10205 | rlogin Service Detection |
| HIGH | 7.5* | 6.7 | 10245 | rsh Service Detection |
| MEDIUM | 6.5 | 3.6 | 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 | 6.5 | - | 42263 | Unencrypted Telnet Server |
| MEDIUM | 5.9 | 5.1 | 136808 | ISC BIND Denial of Service |

| | | | | |
|---|---|---|---|---|
| MEDIUM | 5.9 | 3.6 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 4.4 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 3.6 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | - | 12217 | DNS Server Cache Snooping Remote Information Disclosure |
| MEDIUM | 5.3 | 4.0 | 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 | 52611 | SMTP Service STARTTLS Plaintext Command Injection |
| MEDIUM | 4.3* | - | 90317 | SSH Weak Algorithms Supported |
| MEDIUM | 4.3* | 4.5 | 81606 | SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) |
| LOW | 3.7 | - | 153953 | SSH Weak Key Exchange Algorithms Enabled |
| LOW | 3.7 | 4.5 | 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
| LOW | 3.7 | 4.5 | 83738 | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
| LOW | 3.4 | 5.3 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| LOW | 2.6* | 2.5 | 70658 | SSH Server CBC Mode Ciphers Enabled |
| LOW | 2.6* | - | 71049 | SSH Weak MAC Algorithms Enabled |
| LOW | 2.6* | - | 10407 | X Server Detection |
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| 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 | - | 39519 | Backported Security Patch Detection (FTP) |
| INFO | N/A | - | 84574 | Backported Security Patch Detection (PHP) |
| 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 | - | 35373 | DNS Server DNSSEC Aware Resolver |
| INFO | N/A | - | 11002 | DNS Server Detection |
| INFO | N/A | - | 35371 | DNS Server hostname.bind Map Hostname Disclosure |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| 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 | - | 11156 | IRC Daemon Version Detection |
| INFO | N/A | - | 10397 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure |
| 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 (remote 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 | - | 50845 | OpenSSL Detection |
| INFO | N/A | - | 48243 | PHP Version 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 | - | 11819 | TFTP Daemon Detection |
| INFO | N/A | - | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | 10281 | Telnet Server Detection |
| 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

## 192.168.1.95

| 0 | 0 | 0 | 0 | 6 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 6

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| 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

## 192.168.1.130

| 0 | 0 | 0 | 0 | 6 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 6

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| 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

# 192.168.1.141

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 12 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 13

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| INFO | N/A | - | 11219 | Nessus SYN scanner |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 66334 | Patch Report |
| 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

# 192.168.1.167

| | | | | |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 6 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 6

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| 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

## 192.168.1.239

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 12 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 14

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| MEDIUM | 6.5 | 4.9 | 50686 | IP Forwarding Enabled |
| INFO | N/A | - | 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 | - | 11219 | Nessus SYN scanner |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 66334 | Patch Report |
| 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

# 192.168.1.254

| 4 | 2 | 2 | 0 | 50 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 58

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.0 | 9.2 | 156164 | Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution |
| CRITICAL | 10.0 | 10.0 | 156016 | Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| CRITICAL | 10.0 | 10.0 | 156014 | Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP) |
| HIGH | 8.8 | 7.4 | 164017 | NodeJS System Information Library Command Injection (CVE-2021-21315) |
| HIGH | 7.4 | 6.0 | 174697 | OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0 Multiple Vulnerabilities (2023-04-18 |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 6.0 | 180253 | Tenable Nessus < 10.6.0 Multiple Vulnerabilities (TNS-2023-29) |
| INFO | N/A | - | 141394 | Apache HTTP Server Installed (Linux) |
| INFO | N/A | - | 142640 | Apache HTTP Server Site Enumeration |
| INFO | N/A | - | 166602 | Asset Attribute: Fully Qualified Domain Name (FQDN) |
| INFO | N/A | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | 55472 | Device Hostname |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 159273 | Dockerfile Detection for Linux/UNIX |
| INFO | N/A | - | 25203 | Enumerate IPv4 Interfaces via SSH |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 25202 | Enumerate IPv6 Interfaces via SSH |
| INFO | N/A | - | 33276 | Enumerate MAC Addresses via SSH |
| INFO | N/A | - | 170170 | Enumerate the Network Interaface configuration via SSH |
| INFO | N/A | - | 179200 | Enumerate the Network Routing configuration via SSH |
| INFO | N/A | - | 168980 | Enumerate the PATH Variables |
| 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 | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| INFO | N/A | - | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | 171410 | IP Assignment Method Detection |
| INFO | N/A | - | 147817 | Java Detection and Identification (Linux / Unix) |
| INFO | N/A | - | 151883 | Libgcrypt Installed (Linux/UNIX) |
| INFO | N/A | - | 157358 | Linux Mounted Devices |
| INFO | N/A | - | 95928 | Linux User List Enumeration |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 10147 | Nessus Server Detection |
| INFO | N/A | - | 64582 | Netstat Connection Information |
| INFO | N/A | - | 14272 | Netstat Portscanner (SSH) |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 97993 | OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) |
| INFO | N/A | - | 117887 | OS Security Patch Assessment Available |
| INFO | N/A | - | 148373 | OpenJDK Java Detection (Linux / Unix) |
| INFO | N/A | - | 168007 | OpenSSL Installed (Linux) |
| INFO | N/A | - | 66334 | Patch Report |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 130024 | PostgreSQL Client/Server Installed (Linux) |
| INFO | N/A | - | 174788 | SQLite Local Detection (Linux) |
| INFO | N/A | - | 56984 | SSL / TLS Versions Supported |
| INFO | N/A | - | 10863 | SSL Certificate Information |
| INFO | N/A | - | 21643 | SSL Cipher Suites Supported |
| INFO | N/A | - | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | - | 22964 | Service Detection |
| INFO | N/A | - | 22869 | Software Enumeration (SSH) |
| INFO | N/A | - | 42822 | Strict Transport Security (STS) Detection |
| INFO | N/A | - | 136318 | TLS Version 1.2 Protocol Detection |
| INFO | N/A | - | 110095 | Target Credential Issues by Authentication Protocol - No Issues Found |
| INFO | N/A | - | 141118 | Target Credential Status by Authentication Protocol - Valid Credentials Provided |
| INFO | N/A | - | 163326 | Tenable Nessus Installed (Linux) |
| INFO | N/A | - | 56468 | Time of Last System Startup |
| INFO | N/A | - | 110483 | Unix / Linux Running Processes Information |
| INFO | N/A | - | 152742 | Unix Software Discovery Commands Available |
| INFO | N/A | - | 136340 | nginx Installed (Linux/UNIX) |

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