# Meta2

## Vulnerabilities by Host

# Vulnerabilities by Host

# 192.168.1.7

| | | | | | |
|---|---|---|---|---|---|
| 8 | 6 | 17 | 8 | 75 | |
| CRITICAL | HIGH | MEDIUM | LOW | INFO | |
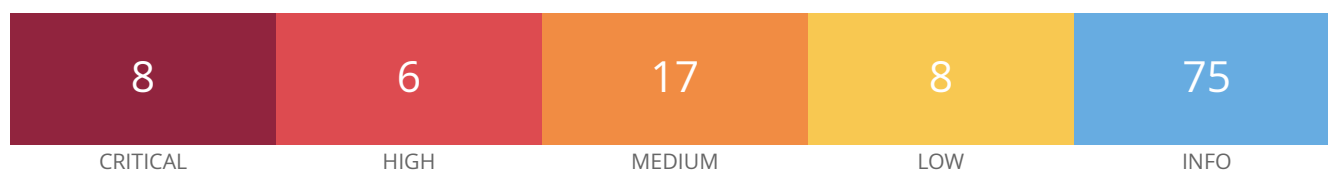
Vulnerabilities

Total: 114

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME |
|---|---|---|---|---|---|
| CRITICAL | 9.8 | 8.9 | 0.9447 | 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 | - | - | 201352 | Canonical Ubuntu Linux SEoL (8.04.x) |
| CRITICAL | 10.0* | 5.1 | 0.0165 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Genera Weakness |
| CRITICAL | 10.0* | 5.1 | 0.0165 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check) |
| CRITICAL | 10.0* | 8.4 | 0.6132 | 46882 | UnrealIRCd Backdoor Detection |
| CRITICAL | 10.0* | - | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.6 | 5.2 | 0.0334 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 5.1 | 0.4002 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 5.9 | 0.7865 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 7.4 | 0.4664 | 10205 | rlogin Service Detection |
| HIGH | 7.5* | 7.4 | 0.4664 | 10245 | rsh Service Detection |
| MEDIUM | 6.5 | 4.4 | 0.0045 | 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 | 4.4 | 0.9238 | 136808 | ISC BIND Denial of Service |
| MEDIUM | 5.9 | 4.4 | 0.027 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 3.6 | 0.8991 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption) |
| MEDIUM | 5.9 | 7.3 | 0.9303 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | 4.0 | 0.8269 | 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* | 7.3 | 0.6128 | 52611 | SMTP Service STARTTLS Plaintext Command Injection |
| MEDIUM | 4.3* | - | - | 90317 | SSH Weak Algorithms Supported |
| MEDIUM | 4.3* | 1.4 | 0.9243 | 81606 | SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREA |
| LOW | 3.7 | 6.5 | 0.0307 | 70658 | SSH Server CBC Mode Ciphers Enabled |
| LOW | 3.7 | - | - | 153953 | SSH Weak Key Exchange Algorithms Enabled |
| LOW | 3.7 | 4.5 | 0.9403 | 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
| LOW | 3.7 | 4.5 | 0.9403 | 83738 | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam) |
| LOW | 3.4 | 5.1 | 0.9424 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| LOW | 2.1* | 2.2 | 0.0037 | 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 | - | - | 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 | - | - | 11002 | DNS Server Detection |
| INFO | N/A | - | - | 72779 | DNS Server Version 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 | - | - | 12053 | Host Fully Qualified Domain Name (FQDN) Resolution |
| 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 | - | - | 209654 | OS Fingerprints Detected |
| 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 | - | - | 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