

**scan meta**

**Nessus Essentials**

Report generated by Nessus™ Thu, 26 Oct 2023 12:15:47 CEST

**TABLE OF CONTENTS**

[**Vulnerabilities by Host**](#_bookmark0)

* [192.168.50.101........................................................................................................................................................... 4](#_bookmark1)

**Nessus Essentials**

**Vulnerabilities by Host**

**Nessus Essentials**

**192.168.50.101**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 4 | 16 | 6 | 68 |

CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 102

**Nessus Essentials**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **SEVERITY** | **CVSS V3.0** | **VPR SCORE** | **PLUGIN** | **NAME** |
|  |  |  |  |  |  |
|  | CRITICAL | 9.8 | 9.0 | [134862](https://www.tenable.com/plugins/nessus/134862) | Apache Tomcat A JP Connector Request Injection (Ghostcat) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 9.8 | - | [51988](https://www.tenable.com/plugins/nessus/51988) | Bind Shell Backdoor Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 9.8 | - | [20007](https://www.tenable.com/plugins/nessus/20007) | SSL Version 2 and 3 Protocol Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0 | - | [33850](https://www.tenable.com/plugins/nessus/33850) | Unix Operating System Unsupported Version Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0\* | 7.4 | [32314](https://www.tenable.com/plugins/nessus/32314) | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  |  |  |  | Weakness |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0\* | 7.4 | [32321](https://www.tenable.com/plugins/nessus/32321) | Debian OpenSSH/OpenSSL Package Random Number Generator |
|  |  |  |  |  | Weakness (SSL check) |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0\* | 5.9 | [11356](https://www.tenable.com/plugins/nessus/11356) | NFS Exported Share Information Disclosure |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0\* | - | [61708](https://www.tenable.com/plugins/nessus/61708) | VNC Server 'password' Password |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | HIGH | 8.6 | 5.2 | [136769](https://www.tenable.com/plugins/nessus/136769) | ISC BIND Service Downgrade / Reflected DoS |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | HIGH | 7.5 | - | [42256](https://www.tenable.com/plugins/nessus/42256) | NFS Shares World Readable |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | HIGH | 7.5 | 6.1 | [42873](https://www.tenable.com/plugins/nessus/42873) | SSL Medium Strength Cipher Suites Supported (SWEET32) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | HIGH | 7.5 | 6.7 | [90509](https://www.tenable.com/plugins/nessus/90509) | Samba Badlock Vulnerability |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | MEDIUM | 6.5 | 3.6 | [139915](https://www.tenable.com/plugins/nessus/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](https://www.tenable.com/plugins/nessus/51192) | SSL Certificate Cannot Be Trusted |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | MEDIUM | 6.5 | - | [57582](https://www.tenable.com/plugins/nessus/57582) | SSL Self-Signed Certificate |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | MEDIUM | 6.5 | - | [104743](https://www.tenable.com/plugins/nessus/104743) | TLS Version 1.0 Protocol Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | MEDIUM | 5.9 | 5.1 | [136808](https://www.tenable.com/plugins/nessus/136808) | ISC BIND Denial of Service |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | MEDIUM | 5.9 | 3.6 | [31705](https://www.tenable.com/plugins/nessus/31705) | SSL Anonymous Cipher Suites Supported |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MEDIUM | 5.9 | 4.4 | [89058](https://www.tenable.com/plugins/nessus/89058) | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 4.4 | [65821](https://www.tenable.com/plugins/nessus/65821) | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | 4.0 | [11213](https://www.tenable.com/plugins/nessus/11213) | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.3 | - | [57608](https://www.tenable.com/plugins/nessus/57608) | SMB Signing not required |
| MEDIUM | 5.3 | - | [15901](https://www.tenable.com/plugins/nessus/15901) | SSL Certificate Expiry |
| MEDIUM | 5.3 | - | [45411](https://www.tenable.com/plugins/nessus/45411) | SSL Certificate with Wrong Hostname |
| MEDIUM | 5.3 | - | [26928](https://www.tenable.com/plugins/nessus/26928) | SSL Weak Cipher Suites Supported |
| MEDIUM | 4.0\* | 6.3 | [52611](https://www.tenable.com/plugins/nessus/52611) | SMTP Service STARTTLS Plaintext Command Injection |
| MEDIUM | 4.3\* | - | [90317](https://www.tenable.com/plugins/nessus/90317) | SSH Weak Algorithms Supported |
| MEDIUM | 4.3\* | 4.5 | [81606](https://www.tenable.com/plugins/nessus/81606) | SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK) |
| LOW | 3.7 | - | [153953](https://www.tenable.com/plugins/nessus/153953) | SSH Weak Key Exchange Algorithms Enabled |
| LOW | 3.7 | 4.5 | [83738](https://www.tenable.com/plugins/nessus/83738) | SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
| LOW | 3.4 | 5.3 | [78479](https://www.tenable.com/plugins/nessus/78479) | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| LOW | 2.6\* | 6.5 | [70658](https://www.tenable.com/plugins/nessus/70658) | SSH Server CBC Mode Ciphers Enabled |
| LOW | 2.6\* | - | [71049](https://www.tenable.com/plugins/nessus/71049) | SSH Weak MAC Algorithms Enabled |
| LOW | 2.6\* | - | [10407](https://www.tenable.com/plugins/nessus/10407) | X Server Detection |
| INFO | N/A | - | [10114](https://www.tenable.com/plugins/nessus/10114) | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | [10223](https://www.tenable.com/plugins/nessus/10223) | RPC portmapper Service Detection |
| INFO | N/A | - | [21186](https://www.tenable.com/plugins/nessus/21186) | A JP Connector Detection |
| INFO | N/A | - | [18261](https://www.tenable.com/plugins/nessus/18261) | Apache Banner Linux Distribution Disclosure |
| INFO | N/A | - | [48204](https://www.tenable.com/plugins/nessus/48204) | Apache HTTP Server Version |
| INFO | N/A | - | [84574](https://www.tenable.com/plugins/nessus/84574) | Backported Security Patch Detection (PHP) |
| INFO | N/A | - | [39520](https://www.tenable.com/plugins/nessus/39520) | Backported Security Patch Detection (SSH) |
| INFO | N/A | - | [39521](https://www.tenable.com/plugins/nessus/39521) | Backported Security Patch Detection (WWW) |

N/A - [45590](https://www.tenable.com/plugins/nessus/45590) Common Platform Enumeration (CPE)

INFO

INFO

N/A - [10028](https://www.tenable.com/plugins/nessus/10028) DNS Server BIND version Directive Remote Version Detection N/A - [11002](https://www.tenable.com/plugins/nessus/11002) DNS Server Detection

N/A - [35371](https://www.tenable.com/plugins/nessus/35371) DNS Server hostname.bind Map Hostname Disclosure N/A - [54615](https://www.tenable.com/plugins/nessus/54615) Device Type

INFO

INFO

INFO

INFO

N/A - [10092](https://www.tenable.com/plugins/nessus/10092) FTP Server Detection

INFO

N/A - [10107](https://www.tenable.com/plugins/nessus/10107) HTTP Server Type and Version

N/A - [24260](https://www.tenable.com/plugins/nessus/24260) HyperText Transfer Protocol (HTTP) Information N/A - [11156](https://www.tenable.com/plugins/nessus/11156) IRC Daemon Version Detection

INFO

INFO

INFO

N/A - [10397](https://www.tenable.com/plugins/nessus/10397) Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

INFO

N/A - [10785](https://www.tenable.com/plugins/nessus/10785) Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

N/A - [11011](https://www.tenable.com/plugins/nessus/11011) Microsoft Windows SMB Service Detection

INFO

INFO

N/A - [100871](https://www.tenable.com/plugins/nessus/100871) Microsoft Windows SMB Versions Supported (remote check)

N/A - [106716](https://www.tenable.com/plugins/nessus/106716) Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO

INFO

N/A - [10437](https://www.tenable.com/plugins/nessus/10437) NFS Share Export List N/A - [11219](https://www.tenable.com/plugins/nessus/11219) Nessus SYN scanner

N/A - [19506](https://www.tenable.com/plugins/nessus/19506) Nessus Scan Information N/A - [11936](https://www.tenable.com/plugins/nessus/11936) OS Identification

INFO

INFO

INFO

INFO

N/A - [117886](https://www.tenable.com/plugins/nessus/117886) OS Security Patch Assessment Not Available N/A - [181418](https://www.tenable.com/plugins/nessus/181418) OpenSSH Detection

INFO

INFO

N/A - [50845](https://www.tenable.com/plugins/nessus/50845) OpenSSL Detection N/A - [48243](https://www.tenable.com/plugins/nessus/48243) PHP Version Detection N/A - [66334](https://www.tenable.com/plugins/nessus/66334) Patch Report

INFO

INFO

INFO

N/A - [118224](https://www.tenable.com/plugins/nessus/118224) PostgreSQL STARTTLS Support

N/A - [26024](https://www.tenable.com/plugins/nessus/26024) PostgreSQL Server Detection N/A - [22227](https://www.tenable.com/plugins/nessus/22227) RMI Registry Detection

INFO

INFO

INFO

N/A - [11111](https://www.tenable.com/plugins/nessus/11111) RPC Services Enumeration N/A - [53335](https://www.tenable.com/plugins/nessus/53335) RPC portmapper (TCP) N/A - [10263](https://www.tenable.com/plugins/nessus/10263) SMTP Server Detection

INFO

INFO

INFO

N/A - [42088](https://www.tenable.com/plugins/nessus/42088) SMTP Service STARTTLS Command Support N/A - [70657](https://www.tenable.com/plugins/nessus/70657) SSH Algorithms and Languages Supported N/A - [149334](https://www.tenable.com/plugins/nessus/149334) SSH Password Authentication Accepted N/A - [10881](https://www.tenable.com/plugins/nessus/10881) SSH Protocol Versions Supported

INFO

INFO

INFO

INFO

N/A - [153588](https://www.tenable.com/plugins/nessus/153588) SSH SHA-1 HMAC Algorithms Enabled N/A - [10267](https://www.tenable.com/plugins/nessus/10267) SSH Server Type and Version Information N/A - [56984](https://www.tenable.com/plugins/nessus/56984) SSL / TLS Versions Supported

INFO

INFO

INFO

N/A - [45410](https://www.tenable.com/plugins/nessus/45410) SSL Certificate 'commonName' Mismatch N/A - [10863](https://www.tenable.com/plugins/nessus/10863) SSL Certificate Information

INFO

INFO

N/A - [70544](https://www.tenable.com/plugins/nessus/70544) SSL Cipher Block Chaining Cipher Suites Supported N/A - [21643](https://www.tenable.com/plugins/nessus/21643) SSL Cipher Suites Supported

INFO

INFO

N/A - [62563](https://www.tenable.com/plugins/nessus/62563) SSL Compression Methods Supported

INFO

N/A - [57041](https://www.tenable.com/plugins/nessus/57041) SSL Perfect Forward Secrecy Cipher Suites Supported N/A - [51891](https://www.tenable.com/plugins/nessus/51891) SSL Session Resume Supported

N/A - [156899](https://www.tenable.com/plugins/nessus/156899) SSL/TLS Recommended Cipher Suites N/A - [25240](https://www.tenable.com/plugins/nessus/25240) Samba Server Detection

INFO

INFO

INFO

INFO

N/A - [104887](https://www.tenable.com/plugins/nessus/104887) Samba Version

INFO

N/A - [96982](https://www.tenable.com/plugins/nessus/96982) Server Message Block (SMB) Protocol Version 1 Enabled

(uncredentialed check) N/A - [22964](https://www.tenable.com/plugins/nessus/22964) Service Detection

INFO

INFO

N/A - [17975](https://www.tenable.com/plugins/nessus/17975) Service Detection (GET request)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| INFO | N/A | - | [25220](https://www.tenable.com/plugins/nessus/25220) | TCP/IP Timestamps Supported |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [110723](https://www.tenable.com/plugins/nessus/110723) | Target Credential Status by Authentication Protocol - No Credentials |
|  |  |  |  | Provided |
|  |  |  |  |  |
| INFO | N/A | - | [10287](https://www.tenable.com/plugins/nessus/10287) | Traceroute Information |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [11154](https://www.tenable.com/plugins/nessus/11154) | Unknown Service Detection: Banner Retrieval |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [19288](https://www.tenable.com/plugins/nessus/19288) | VNC Server Security Type Detection |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [65792](https://www.tenable.com/plugins/nessus/65792) | VNC Server Unencrypted Communication Detection |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [10342](https://www.tenable.com/plugins/nessus/10342) | VNC Software Detection |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [135860](https://www.tenable.com/plugins/nessus/135860) | WMI Not Available |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [11424](https://www.tenable.com/plugins/nessus/11424) | WebDAV Detection |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [10150](https://www.tenable.com/plugins/nessus/10150) | Windows NetBIOS / SMB Remote Host Information Disclosure |
|  |  |  |  |  |
|  |  |  |  |  |
| INFO | N/A | - | [52703](https://www.tenable.com/plugins/nessus/52703) | vsftpd Detection |
|  |  |  |  |  |

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

Parlando delle vulnerabilità critiche, possiamo prendere le seguenti ed analizzarle:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | CRITICAL | 9.8 | 9.0 | [134862](https://www.tenable.com/plugins/nessus/134862) | Apache Tomcat A JP Connector Request Injection (Ghostcat) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 9.8 | - | [51988](https://www.tenable.com/plugins/nessus/51988) | Bind Shell Backdoor Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 9.8 | - | [20007](https://www.tenable.com/plugins/nessus/20007) | SSL Version 2 and 3 Protocol Detection |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | CRITICAL | 10.0 | - | [33850](https://www.tenable.com/plugins/nessus/33850) | Unix Operating System Unsupported Version Detection |

La prima vulnerabilità riguarda un APACHE AJP connector. APACHE è un server web che può operare su diversi sistemi operativi, compreso Linux. Un attaccante potrebbe facilmente sfruttare questa vulnerabilità per arrivare ad eludere la sicurezza del nostro client basandosi sul nostro indirizzo IP. Per porre rimedio, sarà sufficiente fare un aggiornamento della configurazione AJP.

La seconda vulnerabilità, invece, fa riferimento ad una backdoor presente in una shell del nostro Sistema. Dovremo quindi assicurarci che il nostro host non sia compromesso e, nel caso lo fosse, reinstallre il Sistema per provare a neutralizzare questa vulnerabilità in quanto un attaccante potrebbe sfruttare la stessa per introdursi nel nostro sistema e lanciare direttamente comandi.

Riguardo la terza vulnerabilità, sappiamo che riguarda il certificato x509 del protocollo SSL (protocollo che permette la trasmissione sicura e criptata di informazioni. Tale certificato presenta un bug nella generazione randomica dei numeri. Questo potrebbe permettere ad un attaccante di scoprire parte della chiave di trasmissione e di effettuare quindi un attacco “man in the middle”. Si consiglia pertanto di generare da zero tutte le chiavi crittografate riguardante SSL.

L’ultima vulnerabilità, infine, riguarda il sistema UNIX persente sul nostro Host. Il sistema non è più supportato in quanto non viene più aggiornato. Essendo una versione vecchia, pertanto, un soggetto ostile potrebbe facilmente sfruttare le vecchie vulnerabilità per effettuare un attacco. Si consiglia pertanto di passare ad una versione attualmente supportata di Unix.