# Nessus Report

## Nessus Scan Report

Mon, 20 Jan 2020 15:06:59 GMT

# Table Of Contents

# Hosts Summary (Executive)

## 192.168.23.3

### Summary

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 5 | 20 | 20 | 0 | 48 | 93 |

### Details

| Severity | Plugin Id | Name |
|---|---|---|
| Critical (10.0) | 17141 | fingerd Remote Overflow |
| Critical (10.0) | 25217 | Samba < 3.0.25 Multiple Vulnerabilities |
| Critical (10.0) | 58662 | Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows |
| Critical (10.0) | 76314 | Samba Unsupported Version Detection |
| Critical (10.0) | 90508 | Samba 3.x < 4.2.10 / 4.2.x < 4.2.10 / 4.3.x < 4.3.7 / 4.4.x < 4.4.1 Multiple Vulnerabilities (Badlock) |
| High (9.3) | 28228 | Samba < 3.0.27 Multiple Vulnerabilities |
| High (9.3) | 29253 | Samba < 3.0.28 send_mailslot Function Remote Buffer Overflow |
| High (8.5) | 100995 | Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities |
| High (8.5) | 101788 | Apache 2.4.x < 2.4.27 Multiple Vulnerabilities |
| High (7.8) | 10204 | Microsoft Windows NT SCM Malformed Resource Enumeration Request DoS |
| High (7.8) | 55976 | Apache HTTP Server Byte Range DoS |
| High (7.8) | 89080 | Squid 3.x < 3.5.15 / 4.x < 4.0.7 Multiple DoS |
| High (7.8) | 93194 | OpenSSH < 7.3 Multiple Vulnerabilities |
| High (7.8) | 93865 | ISC BIND 9.9.x < 9.9.9-P3 / 9.10.x < 9.10.4-P3 / 9.11.x < 9.11.0rc3 buffer.c Query Response DoS |
| High (7.8) | 96451 | Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy) |
| High (7.8) | 96625 | ISC BIND 9 < 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2 Multiple DoS |
| High (7.8) | 99478 | ISC BIND 9 < 9.9.9-P8 / 9.9.9-S10 / 9.9.10rc3 / 9.10.4-P8 / 9.10.5rc3 / 9.11.0-P5 / 9.11.1r3 Multiple Vunlerabilities |
| High (7.8) | 101232 | ISC BIND 9 < 9.9.10-P2 / 9.9.10-S3 / 9.10.5-P2 / 9.10.5-S3 / 9.11.1-P2 Multiple Vulnerabilities |
| High (7.5) | 24685 | Samba < 3.0.24 Multiple Flaws |
| High (7.5) | 32476 | Samba < 3.0.30 receive_smb_raw Function Remote Buffer Overflow |
| High (7.5) | 47036 | Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption |
| High (7.5) | 49228 | Samba 3.x < 3.5.5 / 3.4.9 / 3.3.14 sid_parse Buffer Overflow |
| High (7.2) | 100996 | ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1-P1 Multiple Vulnerabilities |

| | | |
|---|---|---|
| High (7.1) | 92493 | ISC BIND 9.x < 9.9.9-P2 / 9.10.x < 9.10.4-P2 / 9.11.0a3 < 9.11.0b2 lwres Query DoS |
| High (7.1) | 97227 | ISC BIND 9 < 9.9.9-P6 / 9.9.9-S8 / 9.10.4-P6 / 9.11.0-P3 DNS64 and RPZ DoS |
| Medium (6.9) | 96151 | OpenSSH < 7.4 Multiple Vulnerabilities |
| Medium (6.8) | 55733 | Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities |
| Medium (6.8) | 90509 | Samba Badlock Vulnerability |
| Medium (6.8) | 91193 | Squid 3.x < 3.5.17 / 4.x < 4.0.9 Esi.cc Multiple Vulnerabilities |
| Medium (6.8) | 91194 | Squid 2.x / 3.x < 3.5.17 / 4.x < 4.0.9 cachemgr.cgi RCE |
| Medium (6.0) | 41970 | Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities |
| Medium (5.8) | 42263 | Unencrypted Telnet Server |
| Medium (5.1) | 64459 | Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple Vulnerabilities |
| Medium (5.0) | 11613 | Check Point FireWall-1/VPN-1 Syslog Daemon Remote Overflow DoS |
| Medium (5.0) | 12217 | DNS Server Cache Snooping Remote Information Disclosure |
| Medium (5.0) | 12218 | mDNS Detection (Remote Network) |
| Medium (5.0) | 35450 | DNS Server Spoofed Request Amplification DDoS |
| Medium (5.0) | 52503 | Samba 3.x < 3.3.15 / 3.4.12 / 3.5.7 'FD_SET' Memory Corruption |
| Medium (5.0) | 57608 | SMB Signing Disabled |
| Medium (5.0) | 88099 | Web Server HTTP Header Information Disclosure |
| Medium (5.0) | 99359 | OpenSSH < 7.5 |
| Medium (5.0) | 100617 | Squid 3.5.x < 3.5.23 / 4.x < 4.0.17 Multiple Vulnerabilities |
| Medium (5.0) | 103838 | Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed) |
| Medium (4.3) | 69276 | Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read_nttrans_ea_lis DoS |
| Medium (4.0) | 103781 | OpenSSH < 7.6 |
| Info | 10028 | DNS Server BIND version Directive Remote Version Detection |
| Info | 10052 | Daytime Service Detection |
| Info | 10092 | FTP Server Detection |
| Info | 10107 | HTTP Server Type and Version |
| Info | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| Info | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| Info | 10267 | SSH Server Type and Version Information |
| Info | 10281 | Telnet Server Detection |
| Info | 10287 | Traceroute Information |

| | | |
|---|---|---|
| Info | 10386 | Web Server No 404 Error Code Check |
| Info | 10394 | Microsoft Windows SMB Log In Possible |
| Info | 10397 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure |
| Info | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| Info | 10881 | SSH Protocol Versions Supported |
| Info | 11002 | DNS Server Detection |
| Info | 11011 | Microsoft Windows SMB Service Detection |
| Info | 11040 | HTTP Reverse Proxy Detection |
| Info | 11153 | Service Detection (HELP Request) |
| Info | 11219 | Nessus SYN scanner |
| Info | 11919 | HMAP Web Server Fingerprinting |
| Info | 11936 | OS Identification |
| Info | 11951 | DNS Server Fingerprinting |
| Info | 12264 | Record Route |
| Info | 14788 | IP Protocols Scan |
| Info | 18261 | Apache Banner Linux Distribution Disclosure |
| Info | 19506 | Nessus Scan Information |
| Info | 21745 | Authentication Failure - Local Checks Not Run |
| Info | 22964 | Service Detection |
| Info | 24260 | HyperText Transfer Protocol (HTTP) Information |
| Info | 25220 | TCP/IP Timestamps Supported |
| Info | 25240 | Samba Server Detection |
| Info | 35371 | DNS Server hostname.bind Map Hostname Disclosure |
| Info | 35373 | DNS Server DNSSEC Aware Resolver |
| Info | 42822 | Strict Transport Security (STS) Detection |
| Info | 42823 | Non-compliant Strict Transport Security (STS) |
| Info | 43111 | HTTP Methods Allowed (per directory) |
| Info | 45590 | Common Platform Enumeration (CPE) |
| Info | 46180 | Additional DNS Hostnames |
| Info | 49692 | Squid Proxy Version Detection |
| Info | 52703 | vsftpd Detection |

| | | |
|---|---|---|
| Info | 54615 | Device Type |
| Info | 66334 | Patch Report |
| Info | 70657 | SSH Algorithms and Languages Supported |
| Info | 72779 | DNS Server Version Detection |
| Info | 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| Info | 100871 | Microsoft Windows SMB Versions Supported (remote check) |
| Info | 104410 | Authentication Failure(s) for Provided Credentials |
| Info | 104887 | Samba Version |