



# Metasploit

---

Report generated by Tenable Nessus™

Tue, 04 Feb 2025 23:21:55 India Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.168.234.132.....4

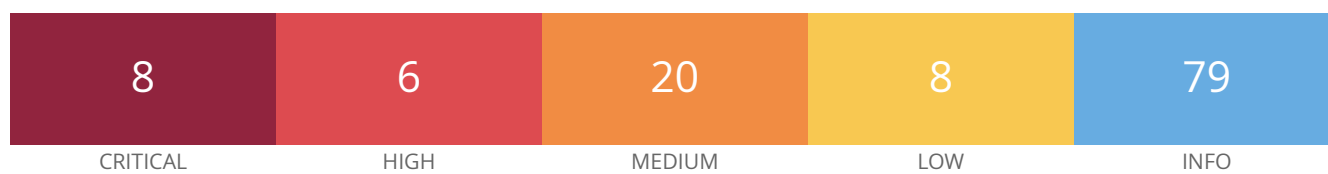
Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.234.132



## Vulnerabilities

Total: 121

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.974	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	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.7565	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0053	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0489	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	0.015	10205	rlogin Service Detection
HIGH	7.5*	6.7	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.2471	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonin
MEDIUM	6.5	4.4	0.004	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	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	<a href="#">42263</a>	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9724	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.003	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.935	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0079	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	-	<a href="#">12217</a>	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	0.0225	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.0135	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREEBIE)
LOW	3.7	6.5	0.498	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	0.9689	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	0.9689	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9744	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.8939	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	<a href="#">10407</a>	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	-	-	39446	Apache Tomcat Detection
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	-	-	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	-	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	<a href="#">10719</a>	MySQL Server Detection
INFO	N/A	-	-	<a href="#">10437</a>	NFS Share Export List
INFO	N/A	-	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">118224</a>	PostgreSQL STARTTLS Support
INFO	N/A	-	-	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	-	-	<a href="#">22227</a>	RMI Registry Detection
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="#">10263</a>	SMTP Server Detection
INFO	N/A	-	-	<a href="#">42088</a>	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	<a href="#">10267</a>	SSH Server Type and Version Information
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="#">62563</a>	SSL Compression Methods Supported
INFO	N/A	-	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">17975</a>	Service Detection (GET request)
INFO	N/A	-	-	<a href="#">11153</a>	Service Detection (HELP Request)
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">11819</a>	TFTP Daemon Detection
INFO	N/A	-	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	<a href="#">10281</a>	Telnet Server Detection
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	<a href="#">20094</a>	VMware Virtual Machine Detection
INFO	N/A	-	-	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	-	-	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available



INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
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