



Remote Vulnerability Testing

Report generated by Tenable Nessus™

Fri, 28 Feb 2025 01:28:01 EST

TABLE OF CONTENTS

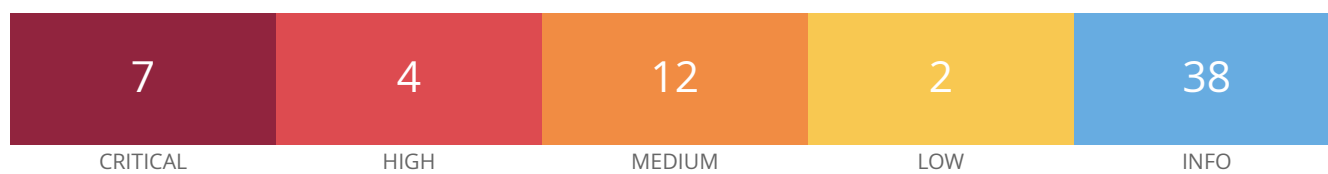
Vulnerabilities by Host

• 192.168.1.125.....	4
----------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.1.125



Vulnerabilities

Total: 63

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	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.2056	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.2056	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	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	4.4	0.0056	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
HIGH	7.5	5.9	0.0489	90509	Samba Badlock Vulnerability
MEDIUM	6.8	6.0	0.2471	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonir
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	5.9	4.4	0.9724	136808	ISC BIND Denial of Service
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	12217	DNS Server Cache Snooping Remote Information Disclosure

MEDIUM	5.3	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
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	0.0135	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	3.4	5.1	0.9744	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
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	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
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	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
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	-	-	52703	vsftpd Detection

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