tenable Nessus

Report generated by Tenable Nessus™

kioptix -1

Sat, 13 Dec 2025 22:03:22 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.114

17	30	40	12	51
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	9.8	6.7	0.6855	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0004	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.6704	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0041	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	7.4	0.4697	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9422	77823	Bash Remote Code Execution (Shellshock)
CRITICAL	9.8	6.7	0.0218	90022	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass
CRITICAL	9.8	8.0	0.8776	17746	OpenSSL 0.9.6 < 0.9.6e Multiple Vulnerabilities
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	5.2	0.0103	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.1	5.2	0.0879	11793	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
CRITICAL	9.0	7.3	0.2314	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	0.9443	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	171347	Apache HTTP Server SEoL (<= 1.3.x)
CRITICAL	10.0*	8.4	0.0071	10883	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
CRITICAL	10.0*	6.7	0.6484	11031	OpenSSH < 3.4 Multiple Remote Overflows
CRITICAL	10.0*	6.3	0.3466	11837	OpenSSH < 3.7.1 Multiple Vulnerabilities

HIGH	7.8	5.9	0.9249	93194	OpenSSH < 7.3 Multiple Vulnerabilities
HIGH	7.5	3.6	0.393	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.1194	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0215	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	0.6274	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0035	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.8912	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0343	200203	OpenSSL 0.9.6 < 0.9.6d Vulnerability
HIGH	7.5	4.4	0.432	17748	OpenSSL 0.9.6 < 0.9.6k Multiple Vulnerabilities
HIGH	7.5	6.1	0.4002	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	6.0	0.9133	11137	Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)
HIGH	7.3	4.9	0.9274	31654	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
HIGH	7.3	4.9	0.593	11030	Apache Chunked Encoding Remote Overflow
HIGH	7.3	6.7	0.0224	96151	OpenSSH < 7.4 Multiple Vulnerabilities
HIGH	7.3	6.3	0.0675	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	7.5*	5.3	0.3065	13651	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	7.5*	5.3	0.0378	10771	OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities
HIGH	7.5*	5.2	0.0048	44069	OpenSSH < 2.9.9p1 Resource Limit Bypass
HIGH	7.2*	6.7	0.0017	10823	OpenSSH < 3.0.2 Multiple Vulnerabilities
HIGH	7.5*	5.2	0.006	44072	OpenSSH < 3.2.3 YP Netgroups Authentication Bypass
HIGH	7.5*	5.5	0.0964	11712	OpenSSH < 3.6.2 Reverse DNS Lookup Bypass
HIGH	7.5*	5.5	0.0268	44077	OpenSSH < 4.5 Multiple Vulnerabilities
HIGH	7.5*	5.3	0.0237	44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
HIGH	7.5*	6.3	0.0085	44081	OpenSSH < 5.7 Multiple Vulnerabilities
HIGH	7.5*	5.3	0.046	73079	OpenSSH < 6.6 Multiple Vulnerabilities
HIGH	8.5*	1.4	0.1017	84638	OpenSSH < 6.9 Multiple Vulnerabilities
HIGH	7.5*	6.3	0.0286	10954	OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
HIGH	7.5*	6.6	0.0026	17751	OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability
HIGH	7.5*	5.8	0.0441	17752	OpenSSL < 0.9.7-beta3 Buffer Overflow
HIGH	7.5*	5.5	0.6266	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.8	6.1	0.6004	159491	OpenSSH < 8.0
MEDIUM	6.5	3.3	0.5039	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	6.5	6.1	0.5777	187201	OpenSSH < 9.6 Multiple Vulnerabilities
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	6.4	3.8	0.4399	90023	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection
MEDIUM	6.1	6.7	0.5515	85382	OpenSSH < 7.0 Multiple Vulnerabilities
MEDIUM	5.9	-	-	99359	OpenSSH < 7.5
MEDIUM	5.9	4.4	0.0793	200207	OpenSSL 0.9.6 < 0.9.6i Vulnerability
MEDIUM	5.9	4.7	0.2316	200201	OpenSSL 0.9.6 < 0.9.6j Multiple Vulnerabilities
MEDIUM	5.9	3.6	0.8991	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	7.3	0.9032	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.8	2.4	0.0373	17756	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	5.3	1.4	0.0019	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	5.9	0.0032	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	4.0	0.6899	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	1.4	0.0284	103781	OpenSSH < 7.6
MEDIUM	5.3	4.9	0.8988	159490	OpenSSH < 7.8
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	4.2	0.0815	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.6*	6.1	0.001	44076	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection
MEDIUM	5.0*	5.3	0.0056	44070	OpenSSH < 2.9.9p2 echo simulation Information Disclosure
MEDIUM	6.8*	4.7	0.0086	10802	OpenSSH < 3.0.1 Multiple Flaws
MEDIUM	6.5*	6.1	0.002	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass
MEDIUM	4.0*	1.4	0.0307	44065	OpenSSH < 5.2 CBC Plaintext Disclosure
MEDIUM	6.9*	5.9	0.0248	31737	OpenSSH X11 Forwarding Session Hijacking
MEDIUM	4.3*	4.7	0.2316	11267	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities
MEDIUM	5.0*	4.4	0.0567	17750	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	5.0*	4.4	0.0567	12110	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	5.0*	3.6	0.0019	17759	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	5.1*	5.9	0.0444	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	4.3*	3.6	0.0589	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	5.0*	3.6	0.043	44074	Portable OpenSSH < 3.8p1 Multiple Vulnerabilities
MEDIUM	5.8*	7.4	0.0294	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	4.3*	1.4	0.9194	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

MEDIUM	4.3*	5.9	0.0469	10816	Webalizer < 2.01-09 Multiple XSS
LOW	3.8	2.4	0.0001	234554	OpenSSH < 10.0 DisableForwarding
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	0.939	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.6	4.0	0.0001	269984	OpenSSH < 10.1 / 10.1p1 Multiple Vulnerabilities
LOW	3.4	5.1	0.9402	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	1.2*	5.5	0.0071	44075	OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure
LOW	3.5*	5.5	0.0274	19592	OpenSSH < 4.2 Multiple Vulnerabilities
LOW	1.2*	3.6	0.0002	44080	OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
LOW	2.1*	3.4	0.0006	53841	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	193143	Linux Time Zone Information
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	64582	Netstat Connection Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection

INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	277650	Remote Services Not Using Post-Quantum Ciphers
INFO	N/A	-	-	25221	Remote listeners enumeration (Linux / AIX)
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	-	-	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	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	58768	SSL Resume With Different Cipher Issue
INFO	N/A	-	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	-	53360	SSL Server Accepts Weak Diffie-Hellman Keys
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	278501	Smartbedded Meteobridge Web Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110095	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

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

Hide