



# kioptrix

---

Report generated by Nessus™

Sat, 18 Nov 2023 11:29:12 EST

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 10.0.2.6.....4

---

## Vulnerabilities by Host

---

## 10.0.2.6



### Vulnerabilities

Total: 132

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	<a href="#">158900</a>	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	<a href="#">161948</a>	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.4	<a href="#">172186</a>	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	<a href="#">11915</a>	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	6.7	<a href="#">153584</a>	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	-	<a href="#">20007</a>	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	5.2	<a href="#">11793</a>	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
CRITICAL	9.0	6.5	<a href="#">170113</a>	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	<a href="#">153583</a>	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	<a href="#">171347</a>	Apache httpd SEoL (<= 1.3.x)
CRITICAL	10.0*	7.4	<a href="#">10883</a>	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
CRITICAL	10.0*	6.7	<a href="#">11031</a>	OpenSSH < 3.4 Multiple Remote Overflows
CRITICAL	10.0*	5.5	<a href="#">11837</a>	OpenSSH < 3.7.1 Multiple Vulnerabilities
HIGH	7.5	5.1	<a href="#">183391</a>	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	5.1	<a href="#">35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	6.0	<a href="#">11137</a>	Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)
HIGH	7.3	4.9	<a href="#">31654</a>	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

HIGH	7.3	4.9	<a href="#">11030</a>	Apache Chunked Encoding Remote Overflow
HIGH	7.3	6.3	<a href="#">10882</a>	SSH Protocol Version 1 Session Key Retrieval
HIGH	7.5*	5.3	<a href="#">13651</a>	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	7.5*	5.3	<a href="#">10771</a>	OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities
HIGH	7.2*	5.9	<a href="#">10823</a>	OpenSSH < 3.0.2 Multiple Vulnerabilities
HIGH	7.5*	5.2	<a href="#">44072</a>	OpenSSH < 3.2.3 YP Netgroups Authentication Bypass
HIGH	7.2*	5.9	<a href="#">17702</a>	OpenSSH < 3.6.1p2 Multiple Vulnerabilities
HIGH	7.5*	5.5	<a href="#">11712</a>	OpenSSH < 3.6.2 Reverse DNS Lookup Bypass
HIGH	7.5*	5.5	<a href="#">44077</a>	OpenSSH < 4.5 Multiple Vulnerabilities
HIGH	7.5*	5.3	<a href="#">44078</a>	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
HIGH	7.5*	6.3	<a href="#">10954</a>	OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
HIGH	7.5*	6.6	<a href="#">17751</a>	OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability
HIGH	7.5*	7.0	<a href="#">17746</a>	OpenSSL < 0.9.6e Multiple Vulnerabilities
HIGH	7.5*	5.8	<a href="#">17752</a>	OpenSSL < 0.9.7-beta3 Buffer Overflow
HIGH	9.3*	5.9	<a href="#">17760</a>	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3*	5.9	<a href="#">57459</a>	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5*	6.7	<a href="#">58799</a>	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	7.5*	5.5	<a href="#">12255</a>	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.5	3.3	<a href="#">17696</a>	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	6.5	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM	5.8	2.4	<a href="#">17756</a>	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	5.3	1.4	<a href="#">88098</a>	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	4.0	<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	4.6*	6.1	<a href="#">44076</a>	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection
MEDIUM	6.8*	4.7	<a href="#">10802</a>	OpenSSH < 3.0.1 Multiple Flaws
MEDIUM	6.5*	6.1	<a href="#">44079</a>	OpenSSH < 4.9 'ForceCommand' Directive Bypass
MEDIUM	4.0*	1.4	<a href="#">44065</a>	OpenSSH < 5.2 CBC Plaintext Disclosure
MEDIUM	5.0*	3.6	<a href="#">44073</a>	OpenSSH With OpenPAM DoS
MEDIUM	6.9*	6.0	<a href="#">31737</a>	OpenSSH X11 Forwarding Session Hijacking
MEDIUM	5.0*	5.9	<a href="#">59076</a>	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	5.0*	3.6	<a href="#">17747</a>	OpenSSL < 0.9.6f Denial of Service
MEDIUM	4.3*	4.7	<a href="#">11267</a>	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities
MEDIUM	5.0*	4.4	<a href="#">17748</a>	OpenSSL < 0.9.6k Denial of Service
MEDIUM	5.0*	3.6	<a href="#">17749</a>	OpenSSL < 0.9.6l Denial of Service
MEDIUM	5.0*	4.4	<a href="#">17750</a>	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	5.0*	4.4	<a href="#">12110</a>	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	5.0*	3.4	<a href="#">17759</a>	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	5.8*	4.2	<a href="#">56996</a>	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	5.0*	5.1	<a href="#">17761</a>	OpenSSL < 0.9.8i Denial of Service
MEDIUM	5.8*	4.0	<a href="#">17762</a>	OpenSSL < 0.9.8j Signature Spoofing

MEDIUM	5.0*	3.6	<a href="#">17763</a>	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.1*	5.9	<a href="#">17765</a>	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0*	3.6	<a href="#">58564</a>	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	4.3*	2.7	<a href="#">51892</a>	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	5.0*	3.6	<a href="#">44074</a>	Portable OpenSSH < 3.8p1 Multiple Vulnerabilities
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	5.8*	7.7	<a href="#">42880</a>	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	4.3*	4.5	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3*	5.9	<a href="#">10816</a>	Webalizer < 2.01-09 Multiple XSS
LOW	3.7	1.4	<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	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	1.2*	5.5	<a href="#">44075</a>	OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure
LOW	3.5*	5.5	<a href="#">19592</a>	OpenSSH < 4.2 Multiple Vulnerabilities
LOW	1.2*	3.6	<a href="#">44080</a>	OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
LOW	2.1*	2.7	<a href="#">17754</a>	OpenSSL < 0.9.7f Insecure Temporary File Creation
LOW	2.6*	3.6	<a href="#">64532</a>	OpenSSL < 0.9.8y Multiple Vulnerabilities
LOW	2.1*	3.4	<a href="#">53841</a>	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	<a href="#">10223</a>	RPC portmapper Service Detection

INFO	N/A	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	<a href="#">84502</a>	HSTS Missing From HTTPS Server
INFO	N/A	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
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="#">57323</a>	OpenSSL Version Detection
INFO	N/A	-	<a href="#">66334</a>	Patch Report
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="#">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="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">58768</a>	SSL Resume With Different Cipher Issue
INFO	N/A	-	<a href="#">94761</a>	SSL Root Certification Authority Certificate Information
INFO	N/A	-	<a href="#">53360</a>	SSL Server Accepts Weak Diffie-Hellman Keys
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="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

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