Kioptrix

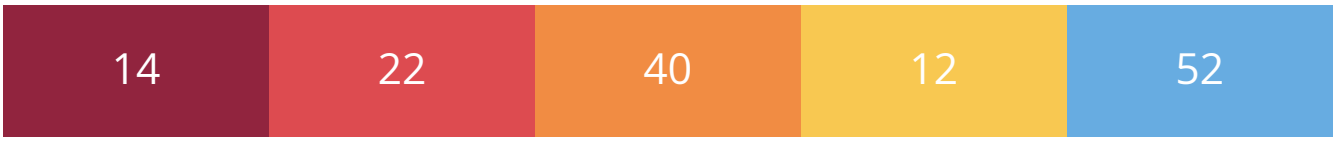
Report generated by Nessus™ Tue, 04 Jul 2023 02:25:24 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.124.135



Vulnerabilities Total: 140

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.4	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	5.2	11793	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
CRITICAL	9.0	7.3	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	171347	Apache httpd SEoL (<= 1.3.x)
CRITICAL	10.0	-	78555	OpenSSL Unsupported
CRITICAL	10.0*	7.4	10883	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
CRITICAL	10.0*	6.7	11031	OpenSSH < 3.4 Multiple Remote Overflows
CRITICAL	10.0*	5.5	11837	OpenSSH < 3.7.1 Multiple Vulnerabilities
HIGH	7.5	5.1	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	6.0	11137	Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)
HIGH	7.3	4.9	31654	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

HIGH	7.3	4.9	11030	Apache Chunked Encoding Remote Overflow
HIGH	7.5*	5.3	13651	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
HIGH	7.5*	5.3	10771	OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities
HIGH	7.2*	5.9	10823	OpenSSH < 3.0.2 Multiple Vulnerabilities
HIGH	7.5*	5.2	44072	OpenSSH < 3.2.3 YP Netgroups Authentication Bypass
HIGH	7.2*	5.9	17702	OpenSSH < 3.6.1p2 Multiple Vulnerabilities
HIGH	7.5*	5.5	11712	OpenSSH < 3.6.2 Reverse DNS Lookup Bypass
HIGH	7.5*	5.5	44077	OpenSSH < 4.5 Multiple Vulnerabilities
HIGH	7.5*	5.3	44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
HIGH	7.5*	6.3	10954	OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
HIGH	7.5*	6.6	17751	OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability
HIGH	7.5*	7.0	17746	OpenSSL < 0.9.6e Multiple Vulnerabilities
HIGH	7.5*	5.8	17752	OpenSSL < 0.9.7-beta3 Buffer Overflow
HIGH	9.3*	5.9	17760	OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH	9.3*	5.9	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5*	6.7	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	7.5*	6.3	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	7.5*	5.5	12255	mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM	6.5	3.3	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
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	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM	5.8	2.4	17756	OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
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	4.6*	6.1	44076	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection
MEDIUM	6.8*	4.7	10802	OpenSSH < 3.0.1 Multiple Flaws
MEDIUM	6.5*	6.1	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass
MEDIUM	4.0*	2.5	44065	OpenSSH < 5.2 CBC Plaintext Disclosure
MEDIUM	5.0*	3.6	44073	OpenSSH With OpenPAM DoS
MEDIUM	6.9*	6.0	31737	OpenSSH X11 Forwarding Session Hijacking
MEDIUM	5.0*	5.9	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	5.0*	3.6	17747	OpenSSL < 0.9.6f Denial of Service
MEDIUM	4.3*	4.7	11267	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities
MEDIUM	5.0*	4.4	17748	OpenSSL < 0.9.6k Denial of Service
MEDIUM	5.0*	3.6	17749	OpenSSL < 0.9.6l Denial of Service
MEDIUM	5.0*	4.4	17750	OpenSSL < 0.9.6m / 0.9.7d Denial of Service
MEDIUM	5.0*	4.4	12110	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS
MEDIUM	5.0*	3.4	17759	OpenSSL < 0.9.8 Weak Default Configuration
MEDIUM	4.3*	4.2	56996	OpenSSL < 0.9.8h Multiple Vulnerabilities
MEDIUM	5.0*	5.1	17761	OpenSSL < 0.9.8i Denial of Service

MEDIUM	5.8*	4.0	17762	OpenSSL < 0.9.8j Signature Spoofing
MEDIUM	5.0*	3.6	17763	OpenSSL < 0.9.8k Multiple Vulnerabilities
MEDIUM	5.1*	5.9	17765	OpenSSL < 0.9.8l Multiple Vulnerabilities
MEDIUM	5.0*	3.6	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	4.3*	2.7	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	5.0*	3.6	44074	Portable OpenSSH < 3.8p1 Multiple Vulnerabilities
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	5.8*	7.7	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3*	5.9	10816	Webalizer < 2.01-09 Multiple XSS
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	1.2*	5.5	44075	OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure
LOW	3.5*	5.5	19592	OpenSSH < 4.2 Multiple Vulnerabilities
LOW	1.2*	3.6	44080	OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
LOW	2.1*	2.7	17754	OpenSSL < 0.9.7f Insecure Temporary File Creation
LOW	2.6*	3.6	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
LOW	2.1*	3.4	53841	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure

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	-	49704	External URLs
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	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
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	-	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	-	153588	SSH SHA-1 HMAC Algorithms Enabled
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	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present

INFO	N/A	-	10662	Web mirroring
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