Kioptrix 1.1

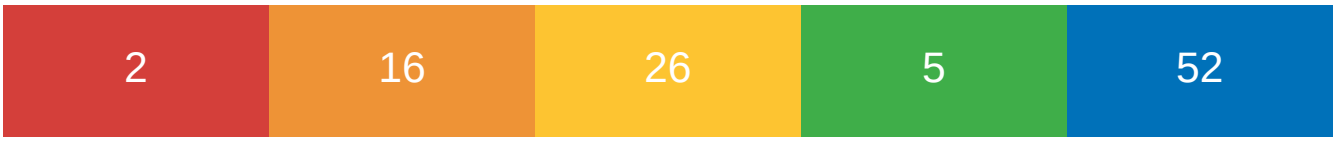
Report generated by Nessus™ Sat, 06 Mar 2021 01:10:39 EST

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.103.143



Vulnerabilities Total: 101

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	9.3	22268	PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities
HIGH	9.3	17710	PHP < 4.4.4 Multiple Vulnerabilities
HIGH	7.5	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	42423	CGI Generic SSI Injection (HTTP headers)
HIGH	7.5	15973	PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities
HIGH	7.5	18033	PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabilities
HIGH	7.5	20111	PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities
HIGH	7.5	24906	PHP < 4.4.5 Multiple Vulnerabilities
HIGH	7.5	29833	PHP < 4.4.8 Multiple Vulnerabilities
HIGH	7.5	33849	PHP < 4.4.9 Multiple Vulnerabilities
HIGH	7.5	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5	57537	PHP < 5.3.9 Multiple Vulnerabilities
HIGH	7.5	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	43351	PHP < 5.2.12 Multiple Vulnerabilities

MEDIUM	6.8	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
MEDIUM	5.4	17687	PHP Multiple Image Processing Functions File Handling DoS
MEDIUM	5.1	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	5.0	40984	Browsable Web Directories
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	35750	PHP < 5.2.9 Multiple Vulnerabilities
MEDIUM	5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	5.0	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	5.0	57640	Web Application Information Disclosure
MEDIUM	4.3	51892	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.6	17709	PHP < 4.4.2 Multiple XSS Vulnerabilities
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
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	14788	IP Protocols Scan
INFO	N/A	117886	Local Checks Not Enabled (info)
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	10719	MySQL Server Detection
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	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)
INFO	N/A	70657	SSH Algorithms and Languages Supported
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	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	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	91815	Web Application Sitemap
INFO	N/A	42057	Web Server Allows Password Auto-Completion
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	49705	Web Server Harvested Email Addresses
INFO	N/A	10662	Web mirroring