Metasploitable scan

Report generated by Nessus™ Tue, 09 Apr 2024 23:32:54 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.69.10

Vulnerabilities Total: 119

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.8	81510	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)
CRITICAL	9.8	8.8	82025	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities
CRITICAL	9.8	6.7	83033	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities
CRITICAL	9.8	6.7	83517	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities
CRITICAL	9.8	6.7	84362	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities
CRITICAL	9.8	5.9	84671	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)
CRITICAL	9.8	7.4	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	5.9	66585	PHP 5.4.x < 5.4.13 Information Disclosure
HIGH	7.3	5.9	69401	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities
HIGH	7.3	6.7	81080	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities
HIGH	7.3	3.6	85298	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities
HIGH	7.3	6.7	85885	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities
HIGH	7.5*	7.4	78515	Drupal Database Abstraction API SQLi
HIGH	9.3*	-	67260	PHP 5.4.x < 5.4.17 Buffer Overflow

HIGH	7.5*	6.7	71427	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption
HIGH	7.2*	6.7	73862	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation
HIGH	7.5*	5.9	76281	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities
HIGH	7.5*	6.7	78545	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities
HIGH	7.5*	6.6	80330	PHP 5.4.x < 5.4.36 'process_nested_data' RCE
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
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	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	6.7	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	2.2	64993	PHP 5.4.x < 5.4.12 Information Disclosure
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	2.9	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	5.0*	3.6	66843	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities
MEDIUM	5.0*	4.4	71927	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	72881	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities
MEDIUM	5.0*	4.2	73338	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS
MEDIUM	5.0*	3.6	74291	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities
MEDIUM	6.8*	5.9	77402	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	79246	PHP 5.4.x < 5.4.35 'donote' DoS
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure

MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	76791	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	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	-	39519	Backported Security Patch Detection (FTP)
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	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	18638	Drupal Software Detection
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	-	10092	FTP Server Detection
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
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	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
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	-	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	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
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	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	66293	Unix Operating System on Extended Support
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting

INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	17219	phpMyAdmin Detection

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