tenable Nessus

pmvc

Report generated by Nessus™ Wed, 08 May 2024 18:42:23 E. South America Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

200.223.235.41

22	9	8	1	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 64

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	84364	PHP 5.6.x < 5.6.10 Multiple Vulnerabilities
CRITICAL	9.8	5.9	84673	PHP 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)
CRITICAL	9.8	6.7	88694	PHP 5.6.x < 5.6.18 Multiple Vulnerabilities
CRITICAL	9.8	5.9	90008	PHP 5.6.x < 5.6.19 Multiple Vulnerabilities
CRITICAL	9.8	6.7	90361	PHP 5.6.x < 5.6.20 Multiple Vulnerabilities
CRITICAL	9.8	6.7	90921	PHP 5.6.x < 5.6.21 Multiple Vulnerabilities
CRITICAL	9.8	6.7	91898	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities
CRITICAL	9.8	6.7	92555	PHP 5.6.x < 5.6.24 Multiple Vulnerabilities (httpoxy)
CRITICAL	9.8	6.7	93077	PHP 5.6.x < 5.6.25 Multiple Vulnerabilities
CRITICAL	9.8	6.7	93656	PHP 5.6.x < 5.6.26 Multiple Vulnerabilities
CRITICAL	9.8	-	94106	PHP 5.6.x < 5.6.27 Multiple Vulnerabilities
CRITICAL	9.8	5.9	95874	PHP 5.6.x < 5.6.29 Multiple Vulnerabilities
CRITICAL	9.8	6.0	96799	PHP 5.6.x < 5.6.30 Multiple DoS
CRITICAL	9.8	6.7	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	6.7	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	6.7	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	6.7	83035	PHP 5.6.x < 5.6.8 Multiple Vulnerabilities
CRITICAL	9.8	6.7	83519	PHP 5.6.x < 5.6.9 Multiple Vulnerabilities

CRITICAL	9.8	7.4	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	9.1	6.0	88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	8.8	5.9	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	8.6	5.9	86301	PHP 5.6.x < 5.6.14 Multiple Vulnerabilities
HIGH	8.6	5.5	91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities
HIGH	7.5	4.4	94955	PHP 5.6.x < 5.6.28 Multiple Vulnerabilities
HIGH	7.5	4.4	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	8.4	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	4.4	85300	PHP 5.6.x < 5.6.12 Multiple Vulnerabilities
HIGH	7.3	6.7	85887	PHP 5.6.x < 5.6.13 Multiple Vulnerabilities
MEDIUM	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	6.1	3.6	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	4.7	4.4	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
MEDIUM	4.3*	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	49704	External URLs
INFO	N/A	-	84502	HSTS Missing From HTTPS Server

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	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	106658	JQuery Detection
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	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
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	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	11419	Web Server Office File Inventory
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	106375	nginx HTTP Server Detection

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