tenable® Nessus

MetasplitableRemediation

TABLE OF CONTENTS

Vulnerabilities by Host

Nessus Essentials

Vulnerabilities by Host

192.168.2.199

8	9	28	9	82
CRITICAL	HIGH	MEDIUM	LOW	INFO
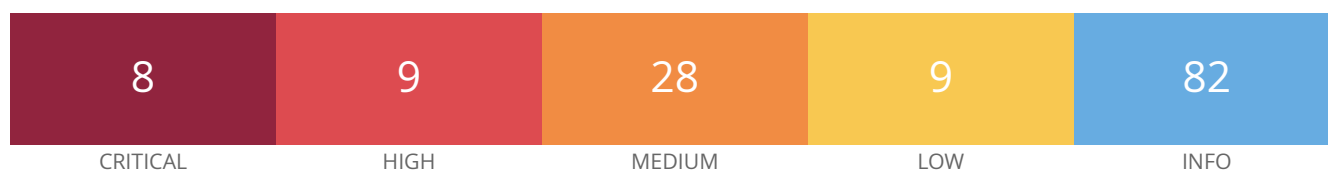
Vulnerabilities   Total: 136

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection

MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
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	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
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	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	39467	CGI Generic Path Traversal
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	5.3	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	11411	Backup Files Disclosure
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	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking

MEDIUM	4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
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	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type

INFO	N/A	-	49704	External URLs
INFO	N/A	-	10092	FTP Server Detection
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	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
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	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	11111	RPC Services Enumeration

INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
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	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume 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	-	17975	Service Detection (GET request)
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	11819	TFTP Daemon Detection

INFO	N/A	-	19941	TWiki Detection
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	19288	VNC Server Security Type Detection
INFO	N/A	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
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	-	11419	Web Server Office File Inventory
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	17219	phpMyAdmin Detection
INFO	N/A	-	52703	vsftpd Detection

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