DPSR_Full_Scan

Report generated by Tenable Nessus™ Sat, 17 May 2025 13:26:08 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

200.0.0.200

Vulnerabilities Total: 138

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabiliti
CRITICAL	9.8	-	-	122060	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities
CRITICAL	9.8	-	-	150280	Apache 2.4.x < 2.4.47 Multiple Vulnerabilities
CRITICAL	9.8	-	-	161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
CRITICAL	9.8	-	-	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	-	-	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	-	-	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	-	-	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	-	-	156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
CRITICAL	9.8	-	-	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	-	-	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentiale check)
CRITICAL	9.8	-	-	89081	OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities
CRITICAL	9.8	-	-	93814	OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities
CRITICAL	9.8	-	-	88694	PHP 5.6.x < 5.6.18 Multiple Vulnerabilities
CRITICAL	9.8	-	-	90008	PHP 5.6.x < 5.6.19 Multiple Vulnerabilities
CRITICAL	9.8	-	-	90361	PHP 5.6.x < 5.6.20 Multiple Vulnerabilities
CRITICAL	9.8	-	-	90921	PHP 5.6.x < 5.6.21 Multiple Vulnerabilities
CRITICAL	9.8	-	-	91898	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities

CRITICAL	9.8	-	-	92555	PHP 5.6.x < 5.6.24 Multiple Vulnerabilities (httpoxy)
CRITICAL	9.8	-	-	93077	PHP 5.6.x < 5.6.25 Multiple Vulnerabilities
CRITICAL	9.8	-	-	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	-	-	95874	PHP 5.6.x < 5.6.29 Multiple Vulnerabilities
CRITICAL	9.8	-	-	96799	PHP 5.6.x < 5.6.30 Multiple DoS
CRITICAL	9.8	-	-	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	-	-	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	-	-	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	-	-	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	-	-	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Exec Vulnerability.
CRITICAL	9.1	-	-	101788	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities
CRITICAL	9.1	-	-	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities
CRITICAL	9.1	-	-	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.1	-	-	88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilit
CRITICAL	9.0	-	-	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	-	-	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	-	-	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remot Code Execution (2509553) (remote check)
HIGH	8.8	-	-	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	8.6	-	-	86301	PHP 5.6.x < 5.6.14 Multiple Vulnerabilities
HIGH	8.6	-	-	91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities
HIGH	8.2	-	-	90890	OpenSSL 1.0.1 < 1.0.1t Multiple Vulnerabilities

HIGH	8.1	-	-	96451	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)
HIGH	8.1	-	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.8	-	-	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
HIGH	7.5	-	-	92320	Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass
HIGH	7.5	-	-	103838	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)
HIGH	7.5	-	-	111788	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities
HIGH	7.5	-	-	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities
HIGH	7.5	-	-	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	-	-	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	-	-	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	-	-	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	-	-	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	-	-	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	-	-	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	-	-	87221	OpenSSL 1.0.1 < 1.0.1q Multiple Vulnerabilities
HIGH	7.5	-	-	88529	OpenSSL 1.0.1 < 1.0.1r Vulnerability
HIGH	7.5	-	-	93112	OpenSSL < 1.0.2i Default Weak 64-bit Block Cipher (SWEET32)
HIGH	7.5	-	-	94955	PHP 5.6.x < 5.6.28 Multiple Vulnerabilities
HIGH	7.5	-	-	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	-	-	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	-	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	-	-	85300	PHP 5.6.x < 5.6.12 Multiple Vulnerabilities
HIGH	7.3	-	-	85887	PHP 5.6.x < 5.6.13 Multiple Vulnerabilities

HIGH	9.3*	-	-	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Rem Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	-	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protoco (3148527) (Badlock) (uncredentialed check)
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 Deprecated Protocol
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	6.1	-	-	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities
MEDIUM	6.1	-	-	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	-	-	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerab
MEDIUM	5.9	-	-	117807	Apache 2.4.x < 2.4.35 DoS
MEDIUM	5.9	-	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	-	-	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	62940	MS12-073: Vulnerabilities in Microsoft IIS Could Allow Informa Disclosure (2733829) (uncredentialed check)
MEDIUM	5.3	-	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.7	-	-	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only
LOW	3.7	-	-	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
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 (remo check)
INFO	N/A	-	-	10719	MySQL Server Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
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	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure

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