Metasploitable

Report generated by Tenable Nessus™ Wed, 04 Dec 2024 16:50:43 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.126.84

Vulnerabilities Total: 88

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9737	197843	Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities
CRITICAL	9.8	6.7	0.0401	111066	Apache Tomcat 7.0.0 < 7.0.89
CRITICAL	9.8	9.0	0.9737	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	7.4	0.9519	175373	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJum
CRITICAL	10.0	-	-	171351	Apache Tomcat SEoL (7.0.x)
HIGH	8.1	9.2	0.9744	103782	Apache Tomcat 7.0.0 < 7.0.82
HIGH	8.1	8.4	0.9752	124064	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities
HIGH	8.1	9.8	0.963	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.1	6.7	0.2633	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.5	6.7	0.0033	197838	Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities
HIGH	7.5	4.4	0.013	197826	Apache Tomcat 7.0.25 < 7.0.90
HIGH	7.5	3.6	0.148	138851	Apache Tomcat 7.0.27 < 7.0.105
HIGH	7.5	3.6	0.0161	121121	Apache Tomcat 7.0.28 < 7.0.88
HIGH	7.5	4.2	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.0	6.7	0.9163	136770	Apache Tomcat 7.0.0 < 7.0.104
HIGH	7.0	5.9	0.0006	147163	Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities

HIGH	7.5*	6.7	0.0004	10483	PostgreSQL Default Unpassworded Account
MEDIUM	6.8	6.0	0.0192	90510	MS16-047: Security Update for SAM and LSAD Remote Protoco (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	4.4	0.0028	106975	Apache Tomcat 7.0.0 < 7.0.85 multiple vulnerabilities
MEDIUM	6.5	4.2	0.8755	10061	Echo Service Detection
MEDIUM	6.5	3.6	0.8755	10198	Quote of the Day (QOTD) Service Detection
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	5.9	3.6	0.0025	148405	Apache Tomcat 7.0.0 < 7.0.107
MEDIUM	5.9	4.4	0.0076	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	1.4	0.0032	106710	Apache Tomcat 7.0.79 < 7.0.84
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.3	2.9	0.8032	118035	Apache Tomcat 7.0.23 < 7.0.91
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only
MEDIUM	5.0*	3.6	0.8755	10043	Chargen UDP Service Remote DoS
LOW	2.1*	4.9	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	10052	Daytime Service Detection
INFO	N/A	-	-	54615	Device Type

INFO	N/A	-	-	11367	Discard Service Detection
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
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	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	174933	Microsoft Message Queuing 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	-	-	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	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	66173	RDP Screenshot
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	56984	SSL / TLS Versions Supported

INFO	N/A	-	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	-	42981	SSL Certificate Expiry - Future Expiry
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	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
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	-	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
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