erp

Report generated by Tenable Nessus™ Sat, 08 Mar 2025 15:29:11 IST

Vulnerabilities by Host

Vulnerabilities by Host

10.40.8.10

Vulnerabilities Total: 65

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9743	133845	Apache Tomcat 9.0.0.M1 < 9.0.31 multiple vulnerabilities
CRITICAL	9.8	9.4	0.0004	213078	Apache Tomcat 9.0.0.M1 < 9.0.98 multiple vulnerabilities
HIGH	7.5	6.7	0.0049	132419	Apache Tomcat 9.0.0.M1 < 9.0.30
HIGH	7.5	4.4	0.0096	138098	Apache Tomcat 9.0.0.M1 < 9.0.36
HIGH	7.5	3.6	0.9123	138591	Apache Tomcat 9.0.0.M1 < 9.0.37 multiple vulnerabilities
HIGH	7.5	4.4	0.0029	144050	Apache Tomcat 9.0.0.M1 < 9.0.40 multiple vulnerabilities
HIGH	7.5	5.9	0.002	147164	Apache Tomcat 9.0.0.M1 < 9.0.43 multiple vulnerabilities
HIGH	7.5	3.6	0.0024	166906	Apache Tomcat 9.0.0.M1 < 9.0.68
HIGH	7.5	4.4	0.0114	171657	Apache Tomcat 9.0.0.M1 < 9.0.71
HIGH	7.5	4.4	0.006	186365	Apache Tomcat 9.0.0.M1 < 9.0.83
HIGH	7.5	3.6	0.0004	201848	Apache Tomcat 9.0.0.M1 < 9.0.90
HIGH	7.5	4.4	0.0854	160894	Apache Tomcat 9.0.13 < 9.0.63
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.0	6.7	0.9331	136806	Apache Tomcat 9.0.0 < 9.0.35
HIGH	7.0	5.9	0.0005	197849	Apache Tomcat 9.0.0.M1 < 9.0.29 multiple vulnerabilities
MEDIUM	6.5	4.2	0.0013	197830	Apache Tomcat 9.0.0.M1 < 9.0.46
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	6.3	4.4	0.0004	192042	Apache Tomcat 9.0.0.M1 < 9.0.86 multiple vulnerabilities
MEDIUM	6.1	3.0	0.0051	180194	Apache Tomcat 9.0.0.M1 < 9.0.80
MEDIUM	5.3	3.6	0.0054	194473	Apache Tomcat 9.0.0.M1 < 9.0.44 multiple vulnerabilities
MEDIUM	5.3	1.4	0.1554	152182	Apache Tomcat 9.0.0.M1 < 9.0.48
MEDIUM	5.3	6.7	0.8556	182809	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.3	1.4	0.0012	141446	Apache Tomcat 9.0.0.M1 < 9.0.38
MEDIUM	4.3	2.2	0.0013	173251	Apache Tomcat 9.0.0.M1 < 9.0.72
LOW	3.7	1.4	0.0015	159464	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell CVE-2021-4398
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
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	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
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 (remo check)

INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
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	-	-	66334	Patch Report
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
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	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
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	-	-	33139	WS-Management Server Detection
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