



scanner-1

Report generated by Nessus™

Tue, 23 Jul 2024 20:50:52 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.50.101.....4

Nessus Essentials

Vulnerabilities by Host

192.168.50.101



Vulnerabilities

Total: 30

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.8	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	106658	JQuery Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
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	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	106375	nginx HTTP Server Detection
INFO	N/A	-	106952	pfSense Detection
INFO	N/A	-	106198	pfSense Web Interface Detection

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