



Orchidhomez

Report generated by Nessus™

Mon, 16 Oct 2023 19:43:54 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

• 68.178.145.172.....	4
-----------------------	---

Nessus Essentials

Vulnerabilities by Host

68.178.145.172



Vulnerabilities

Total: 51

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	54582	SMTP Service Cleartext Login Permitted
LOW	2.6*	6.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10092	FTP Server Detection
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	-	85805	HTTP/2 Cleartext Detection
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	10719	MySQL Server Detection

INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	50350	OS Identification Failed
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	42087	POP3 Service STLS Command Support
INFO	N/A	-	54580	SMTP Authentication Methods
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	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
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	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection

INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	91459	SolarWinds Server & Application Monitor (SAM) Detection
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	11424	WebDAV Detection

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