tenable® Nessus

haseena

Vulnerabilities by Host

Vulnerabilities by Host

0	0	3	0	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities   Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.9	6.1	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
INFO	N/A	-	34098	BIOS Info (SSH)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
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	-	193143	Linux Time Zone Information
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	209654	OS Fingerprints Detected
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10180	Ping the remote host
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	25221	Remote listeners enumeration (Linux / AIX)
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	-	10863	SSL Certificate Information
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	35351	System Information Enumeration (via DMI)
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

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