tenable® Nessus

Task Potato Advanced

Vulnerabilities by Host

Vulnerabilities by Host

10.0.2.11

0	**1**	**2**	**3**	**37**
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities   Total: 43

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
MEDIUM	5.9	6.7	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution

INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10335	Nessus TCP scanner
INFO	N/A	-	11936	OS Identification
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	-	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	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	10662	Web mirroring

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