tenable® Nessus

Scan Bizness

Report generated by Nessus™ Thu, 04 Jul 2024 21:48:16 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.10.11.252

0	1	7	1	53
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 62

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
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	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.3	2.9	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	59245	Apache OFBiz Detection
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	39470	CGI Generic Tests Timeout
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	-	49704	External URLs
INFO	N/A	-	84502	HSTS Missing From HTTPS Server

INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
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	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	106658	JQuery Detection
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
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	-	50845	OpenSSL 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	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information

INFO	N/A	-	159544	SSL Certificate with no Common Name
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	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	62564	TLS Next Protocols Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
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
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	106375	nginx HTTP Server Detection

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