Pentest Tools

SSL/TLS Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform full SSL/TLS scans with more powerful options.

Options	Light scan	Deep scan
Target type	Single host	Multiple hosts
IP range scan	✗	✓
Target SSL port	443	Any port
Target service	HTTPS	• HTTPS • SMTPs • IMAPs • FTPs • and more
SSL port specification	Manual	Auto discovery

✓ djsnetwork.freemyip.com

! The Light SSL/TLS Scanner only checked for port 443. Upgrade to run Deep scansagainst multiple SSL-enabled ports.

Summary

Overall risk level:

Info

Risk ratings:

High:	0
Medium:	0
Low:	0
Info:	19

Scan information:

Start time:	Dec 05, 2024 / 08:25:11 UTC+02
Finish time:	Dec 05, 2024 / 08:29:16 UTC+02
Scan duration:	4 min, 5 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Found 1 open port with SSL/TLS support.

Port	State	Service	Server version	Uses SSL/TLS
443	open	https		Yes

SSL/TLS: Certificate is trusted

port 443/tcp

The domain has been found among Subject Alternate Names (SAN) or is the Common Name (CN) itself.

Therefore, it is considered protected by the certificate.

The Server Name Indication (SNI) has also been found. SNI is an extension to the TLS protocol that allows a client or browser to indicate which hostname it is trying to connect to at the start of the TLS handshake.
This allows the server to present multiple certificates on the same IP address and port number.

SSL/TLS: Certificate is Valid

port 443/tcp

The certificate will expire in 81 days.

SSL/TLS: CA Issuer is invalid or it cannot be identified

port 443/tcp

E6 (let's encrypt from us)

Details

Risk description:
The certificate does not have a valid Certificate Authority Issuer, which are important for checking identity of the owner. Having this risk may result in the browsers not being able to validate the server's identity, compromising the communication between the server and users.

Recommendation:
We recommend you to configure a valid Certificate Authority Issuer for your servers's certificates.

Tested for certificate issues.

port 443/tcp

Certificate number: #1
Issuer: E6 (Let's Encrypt from US)
Signature: ECDSA with SHA384
Serial number: 039A90C2C99B3203F6198D499539BB7ADDCF

SSL/TLS: Not vulnerable to Heartbleed

port 443/tcp

SSL/TLS: Not vulnerable to CCS Injection

port 443/tcp

SSL/TLS: Not vulnerable to Ticketbleed

port 443/tcp

SSL/TLS: Not vulnerable to ROBOT

port 443/tcp

SSL/TLS: Not vulnerable to Secure Renegotiation

port 443/tcp

SSL/TLS: Not vulnerable to CRIME

port 443/tcp

SSL/TLS: Not vulnerable to POODLE

port 443/tcp

SSL/TLS: Not vulnerable to SWEET32

port 443/tcp

SSL/TLS: Not vulnerable to FREAK

port 443/tcp

SSL/TLS: Not vulnerable to DROWN

port 443/tcp

SSL/TLS: Not vulnerable to LOGJAM

port 443/tcp

SSL/TLS: Not vulnerable to BEAST

port 443/tcp

SSL/TLS: Not vulnerable to RC4

port 443/tcp

Tested for SSL/TLS vulnerabilities

port 443/tcp

Scan coverage information

List of tests performed (19/19)

- ✓ Checking for SSL/TLS services...
- ✓ Checking if the certificate is trusted...
- ✓ Checking if the certificate is expired...
- ✓ Checking for Certificate Authority Issuer...
- ✓ Checking the certificate on port 443...
- ✓ Scanning for HEARTBLEED on port 443
- ✓ Scanning for CCS on port 443
- ✓ Scanning for TICKETBLEED on port 443
- ✓ Scanning for ROBOT on port 443
- ✓ Scanning for SECURE_RENEGO on port 443
- ✓ Scanning for CRIME_TLS on port 443
- ✓ Scanning for POODLE_SSL on port 443
- ✓ Scanning for SWEET32 on port 443
- ✓ Scanning for FREAK on port 443
- ✓ Scanning for DROWN on port 443
- ✓ Scanning for LOGJAM on port 443
- ✓ Scanning for BEAST on port 443
- ✓ Scanning for RC4 on port 443
- ✓ Tested for SSL/TLS vulnerabilities

Scan parameters

Target:	djsnetwork.freemyip.com
Preset:	Light
Scanning engines:	Certificate, Vulnerability
Ports to scan:	443