SSL/TLS Vulnerability Scanner Report

✓ vuln.ssl-server.demo

Summary

Overall risk level:

High

Risk ratings:

High:	3
Medium:	3
Low:	0
Info:	8

Scan information:

Start time:	2020-03-18 12:58:16 UTC+02
Finish time:	2020-03-18 12:59:02 UTC+02
Scan duration:	46 sec
Tests performed:	14/14
Scan status:	Finished

Findings

Server certificate is not trusted (port 443)

The certificate of 'k.ro' hasn't got a known issuer.
The certificate has expired.
The certificate's owner does not match hostname 'k.ro'.

Details

Risk description:
The SSL certificate presented by the web server is not trusted by web browsers. This makes it really difficult for humans to distinguish between the real certificate presented by the server and a fake SSL certificate. An attacker could easily mount a man-in-the-middle attack in order to sniff the SSL communication by presenting the user a fake SSL certificate.

Recommendation:
We recommend you to configure a trusted SSL certificate for the web server.

Here are some examples of how to configure SSL for various servers:

- Apache: http://httpd.apache.org/docs/2.2/mod/mod_ssl.html
- Nginx: http://nginx.org/en/docs/http/configuring_https_servers.html

DROWN vulnerability found (port 443)

SSLv2 Offered, But Could Not Detect A Cipher (CVE-2015-3197).
Make Sure You Don'T Use This Certificate Elsewhere, See Https://Censys.Io/Ipv4?Q=2E9A72589Af80Aeb17186A267E20B8244A58E0E778Ed6F97D71B95B60Ecf3F08.

Details

Risk description:
The **DROWN** (Decrypting RSA with Obsolete and Weakened Encryption) attack is a cross-protocol security bug that attacks servers supporting modern SSLv3/TLSprotocol suites by using their support for the obsolete, insecure, SSL v2 protocol to leverage an attack on connections using up-to-date protocols that would otherwise be secure.

Recommendation:
For mitigation, you should disable SSLv2 and make sure to upgrade OpenSSL to a recently released version 1.0.2g and 1.0.1s.

POODLE vulnerability found (port 443)

Uses SSLv3+CBC.

Details

Risk description:
The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in-the-middle context to decipher the

plain text content of an SSLv3 encrypted message.

Recommendation:
To mitigate POODLE, it is recommended to disable SSLv3. For further details visit this guide..

Secure Renegotiation vulnerability found (port 443)

Secure Renegotiation: Vulnerable.

Details

Risk description:
Secure Renegotiation flaw can be exploited by an attacker to send an arbitrary request using the authentication credentials of a victim. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. Also, the attacker can conduct a Denial-of-Service attack by abusing the renegotiation to trigger hundreds of handshakes in the same TCP connection.

Recommendation:
Simple mitigation is to disable SSL renegotiation support on the server.

BEAST vulnerability found (port 443)

Beast: Vulnerable -- And No Higher Protocols As Mitigation Supported.

Details

Risk description:
BEAST, short for Browser Exploit Against SSL/TLS is an attack that leverages weaknesses in cipher block chaining (CBC) to exploit the SSL/TLS protocol. The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.

Recommendation:
To mitigate BEAST, it is recommended to require only TLS 1.1+ ciphers for your server and to reduce the lifespan of the SSL session. More details can be found in this article.

Client-Initiated Secure Renegotiation vulnerability found (port 443)

Secure Client-Initiated Renegotiation : Vulnerable, Dos Threat.

Details

Risk description:
Secure Renegotiation flaw can be exploited by an attacker to send an arbitrary request using the authentication credentials of a victim. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. Also, the attacker can conduct a Denial-of-Service attack by abusing the renegotiation to trigger hundreds of handshakes in the same TCP connection.

Recommendation:
Simple mitigation is to disable SSL renegotiation support on the server.

Found 1 service with SSL/TLS support

Port	State	Service	Server version	Uses SSL/TLS
443	open	https	Apache httpd 1.3.41 ((Unix) mod_fastcgi/2.4.6 mod_ssl/2.8.31 OpenSSL/0.9.7a)	Yes

HTTPS service detected (port 443)

Not vulnerable to LOGJAM (port 443)

Not vulnerable to RC4 (port 443)

Not vulnerable to Heartbleed (port 443)

Not vulnerable to SWEET32 (port 443)

Not vulnerable to Ticketbleed (port 443)

Not vulnerable to FREAK (port 443)

Scan coverage information

List of tests performed (14/14)

- ✓ Checking if SSL/TLS is supported on port 443...
- ✓ Checking for SSL/TLS vulnerabilities on port 443...
- ✓ Checking if server certificate is trusted...
- ✓ Scanning for logjam on port: 443
- ✓ Scanning for rc4 on port: 443
- ✓ Scanning for secure_renego on port: 443
- ✓ Scanning for heartbleed on port: 443
- ✓ Scanning for sweet32 on port: 443
- ✓ Scanning for drown on port: 443
- ✓ Scanning for beast on port: 443
- ✓ Scanning for sec_client_renego on port: 443
- ✓ Scanning for ticketbleed on port: 443
- ✓ Scanning for freak on port: 443
- ✓ Scanning for poodle_ssl on port: 443

Scan parameters

Target:	vuln.ssl-server.demo
Port:	443,
AutoMode:	false