SSL/TLS Vulnerability Scanner Report

81.243.249.45
Vulnerable target IP Address

Summary

Overall risk level:
High

Risk ratings:

High:	5
Medium:	4
Low:	2
Info:	23

Scan information:

Start time:	2023-01-05 15:55:57 UTC+02
Finish time:	2023-01-05 16:01:10 UTC+02
Scan duration:	5 min, 13 sec
Tests performed:	34/34
Scan status:	Finished

Findings

SSL/TLS: POODLE vulnerability found (port 21)

Uses SSLv3+CBC.

Details

Risk description:
The POODLE (Padding Oracle On Downgraded Legacy Encryption) 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.
The POODLE vulnerability is registered in the NIST NVD database asCVE-2014-3566.

Recommendation:
To mitigate POODLE, we recommend disabling SSLv3.
For further details visit the guide https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-poodle-sslv3-vulnerability.

SSL/TLS: Server certificate is not trusted (port 443)

Certificate does not match supplied uri

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

SSL/TLS: Certificate Chain of Trust is incomplete or invalid (port 443)

It looks like the SSL certificate is expired or it is not signed or approved by a company that the browser trusts.

Details

Risk description:
The certificate chain of trust is not complete or is invalid. This misconfiguration has a high propbability to make browsers alert the users that the certificate is not trusted.

Recommendation:
We recommend you to contact your Certificate provider about the chain of trust of your certificates. The most common problem is the Intermediate Certificate not being properly linked to a trusted root authority.

SSL/TLS: Certificate is expired (port 443)

Valid until: 2021-05-14 (expired 1 years, 7 months and 22 days ago)

Details

Risk description:
The SSL certificate presented by the web server is expired. The browsers are not able to properly validate the server's identity, therefore the connection between the user and the browser is not secure.

Recommendation:
We recommend you to contact your Certificate provider and renew your certificate.

SSL/TLS: POODLE vulnerability found (port 443)

Uses SSLv3+CBC.

Details

Risk description:
The POODLE (Padding Oracle On Downgraded Legacy Encryption) 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.
The POODLE vulnerability is registered in the NIST NVD database asCVE-2014-3566.

Recommendation:
To mitigate POODLE, we recommend disabling SSLv3.
For further details visit the guide https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-poodle-sslv3-vulnerability.

SSL/TLS: BEAST vulnerability found (port 21)

Target is vulnerable but it has support for higher protocols: TLSv1.1, TLSv1.2.

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.
The BEAST vulnerability is registered in the NIST NVD database asCVE-2011-3389.

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 at https://community.pivotal.io/s/article/Mitigation-of-CVE-2011-3389-BEAST-for-web-server-administrators-2008784.

SSL/TLS: RC4 vulnerability found (port 21)

Vulnerable ciphers found: RC4-SHA RC4-MD5.

Details

Risk description:
Vulnerabilities in SSL RC4 Cipher Suites are very frequently found on networks around the world. The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic.
The RC4 related vulnerabilities are registered in the NIST NVD database asCVE-2013-2566 and CVE-2015-2808.

Recommendation:
Reconfigure the affected application, if possible, to avoid the use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

SSL/TLS: BEAST vulnerability found (port 443)

Target is vulnerable but it has support for higher protocols: TLSv1.1, TLSv1.2.

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.
The BEAST vulnerability is registered in the NIST NVD database asCVE-2011-3389.

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 at https://community.pivotal.io/s/article/Mitigation-of-CVE-2011-3389-BEAST-for-web-server-administrators-2008784.

SSL/TLS: RC4 vulnerability found (port 443)

Vulnerable ciphers found: RC4-SHA RC4-MD5.

Details

Risk description:
Vulnerabilities in SSL RC4 Cipher Suites are very frequently found on networks around the world. The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic.
The RC4 related vulnerabilities are registered in the NIST NVD database asCVE-2013-2566 and CVE-2015-2808.

Recommendation:
Reconfigure the affected application, if possible, to avoid the use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

SSL/TLS: SWEET32 vulnerability found (port 21)

Uses 64 Bit Block Ciphers.

Details

Risk description:
Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
The SWEET32 vulnerability is registered in the NIST NVD database as

CVE-2016-2183 and
CVE-2016-6329.

Recommendation:
To mitigate SWEET32, you should disable all 3DES Ciphersuites.

SSL/TLS: SWEET32 vulnerability found (port 443)

Uses 64 Bit Block Ciphers.

Details

Risk description:
Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
The SWEET32 vulnerability is registered in the NIST NVD database as
CVE-2016-2183 and
CVE-2016-6329.

Recommendation:
To mitigate SWEET32, you should disable all 3DES Ciphersuites.

SSL/TLS: Found 2 service s with SSL/TLS support

Port	State	Service	Server version	Uses SSL/TLS
21	open	ftp		Yes
443	open	https	2.0	Yes

Tested for certificate issues. (port 443)

Certificate number: #1
Issuer: WEB-SP-LIVE-WEB01-CA (WEB.local)
Signature: SHA256 with RSA
Serial number: 1D00000002D950DFD8A5922BE6000000000002

No SSL certificate has been found (port 21)

Tested for SSL/TLS vulnerabilities (port 21)

SSL/TLS: Not vulnerable to Heartbleed (port 21)

SSL/TLS: Not vulnerable to CCS Injection (port 21)

SSL/TLS: Not vulnerable to ROBOT (port 21)

- SSL/TLS: Not vulnerable to Secure Renegotiation (port 21)
- SSL/TLS: Not vulnerable to CRIME (port 21)
- SSL/TLS: Not vulnerable to FREAK (port 21)
- SSL/TLS: Not vulnerable to DROWN (port 21)
- SSL/TLS: Not vulnerable to LOGJAM (port 21)
- SSL/TLS: Certificate Authority Issuer is valid (port 443)
- Tested for SSL/TLS vulnerabilities (port 443)
- SSL/TLS: Not vulnerable to Heartbleed (port 443)
- SSL/TLS: Not vulnerable to CCS Injection (port 443)
- SSL/TLS: Not vulnerable to Ticketbleed (port 443)
- SSL/TLS: Not vulnerable to ROBOT (port 443)
- SSL/TLS: Not vulnerable to Secure Renegotiation (port 443)
- SSL/TLS: Not vulnerable to CRIME (port 443)
- SSL/TLS: Not vulnerable to FREAK (port 443)
- SSL/TLS: Not vulnerable to DROWN (port 443)
- SSL/TLS: Not vulnerable to LOGJAM (port 443)

Scan coverage information

List of tests performed (34/34)

- ✔ Searching for SSL/TLS services on top 100 TCP ports...
- ✔ Checking the certificate on port 21...
- ✔ Checking for SSL/TLS vulnerabilities on port 21...
- ✔ Scanning for HEARTBLEED on port: 21
- ✔ Scanning for CCS on port: 21
- ✔ Scanning for ROBOT on port: 21
- ✔ Scanning for SECURE_RENEGO on port: 21
- ✔ Scanning for CRIME_TLS on port: 21
- ✔ Scanning for POODLE_SSL on port: 21
- ✔ Scanning for SWEET32 on port: 21
- ✔ Scanning for FREAK on port: 21
- ✔ Scanning for DROWN on port: 21
- ✔ Scanning for LOGJAM on port: 21
- ✔ Scanning for BEAST on port: 21
- ✔ Scanning for RC4 on port: 21
- ✔ Checking the certificate on port 443...
- ✔ Checking if the certificate is trusted...
- ✔ Checking for the certificate chain of trust...
- ✔ Checking if the certificate is expired...
- ✔ Checking for Certificate Authority Issuer...
- ✔ Checking for SSL/TLS vulnerabilities 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

Scan parameters

Target:	81.243.249.45
Port:	443
Auto Detect SSL/TLS:	true