Pentest Tools

SSL/TLS Vulnerability Scanner Report

✓ expired.badssl.com

Summary

Overall risk level:

High

Risk ratings:

Critical:	0
High:	5
Medium:	2
Low:	1
Info:	65

Scan information:

Start time:	Apr 22, 2025 / 18:27:05 UTC+03
Finish time:	Apr 22, 2025 / 18:37:30 UTC+03
Scan duration:	10 min, 25 sec
Tests performed:	73/73
Scan status:	Finished

Findings

SSL/TLS: Certificate is expired or expires within 30 days.

port 443/tcp

Valid until: 2015-04-12 (expired 10 years, and 10 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: Server certificate is not trusted

port 1010/tcp

Certificate does not match supplied uri (same w/o sni)

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 is expired or expires within 30 days.

port 1010/tcp

Valid until: 2018-08-08 (expired 6 years, 8 months and 14 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: Server certificate is not trusted

port 1011/tcp

Certificate does not match supplied uri (same w/o sni)

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 is expired or expires within 30 days.

port 1011/tcp

Valid until: 2018-08-08 (expired 6 years, 8 months and 14 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: BEAST vulnerability found

port 443/tcp

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: BEAST vulnerability found

port 1010/tcp

Vulnerable -- And No Higher Protocols As Mitigation Supported
Vulnerable Ciphers For **CBC Tls1** Detected:
Ecdhe-Rsa-Aes256-Sha Dhe-Rsa-Aes256-Sha Dhe-Rsa-Camellia256-Sha Aes256-Sha Camellia256-Sha Ecdhe-Rsa-Aes128-Sha Dhe-Rsa-Aes128-Sha Dhe-Rsa-Camellia128-Sha Aes128-Sha Camellia128-Sha.

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: SWEET32 vulnerability found

port 443/tcp

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.

Found 7 open ports, 4 with SSL/TLS support.

Port	State	Service	Server version	Uses SSL/TLS
443	open	https	1.10.3	Yes
1012	open	https	1.10.3	Yes
1003	open	https	1.10.3	No
1010	open	https	1.10.3	Yes
1002	open	https	1.10.3	No
1011	open	https	1.10.3	Yes
80	open	http	1.10.3	No

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: CA Issuer is invalid or it cannot be identified

port 443/tcp

Comodo rsa domain validation secure server ca (comodo ca limited from gb)

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: COMODO RSA Domain Validation Secure Server CA (COMODO CA Limited from GB)
Signature: SHA256 with RSA
Serial number: 4AE79549FA9ABE3F100F17A478E16909

SSL/TLS: Certificate is trusted

port 1012/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 1012/tcp

The certificate will expire in 48 days.

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

port 1012/tcp

R10 (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 1012/tcp

Certificate number: #1
Issuer: R10 (Let's Encrypt from US)
Signature: SHA256 with RSA
Serial number: 03B06B8673151255199082F09B2B94A93AF5

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

port 1010/tcp

Badssl intermediate certificate authority (badssl 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 1010/tcp

Certificate number: #1
Issuer: BadSSL Intermediate Certificate Authority (BadSSL from US)
Signature: SHA256 with RSA
Serial number: CDBC5A4AEC9767B1

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

port 1011/tcp

Badssl intermediate certificate authority (badssl 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 1011/tcp

Certificate number: #1
Issuer: BadSSL Intermediate Certificate Authority (BadSSL from US)
Signature: SHA256 with RSA
Serial number: CDBC5A4AEC9767B1

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 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 RC4

port 443/tcp

Tested for SSL/TLS vulnerabilities

port 443/tcp

SSL/TLS: Not vulnerable to Heartbleed

port 1012/tcp

SSL/TLS: Not vulnerable to CCS Injection

port 1012/tcp

SSL/TLS: Not vulnerable to Ticketbleed

port 1012/tcp

SSL/TLS: Not vulnerable to ROBOT

port 1012/tcp

SSL/TLS: Not vulnerable to Secure Renegotiation

port 1012/tcp

SSL/TLS: Not vulnerable to CRIME

port 1012/tcp

SSL/TLS: Not vulnerable to POODLE

port 1012/tcp

SSL/TLS: Not vulnerable to SWEET32

port 1012/tcp

SSL/TLS: Not vulnerable to FREAK

port 1012/tcp

SSL/TLS: Not vulnerable to DROWN

port 1012/tcp

SSL/TLS: Not vulnerable to LOGJAM

port 1012/tcp

SSL/TLS: Not vulnerable to BEAST

port 1012/tcp

SSL/TLS: Not vulnerable to RC4

port 1012/tcp

Tested for SSL/TLS vulnerabilities

port 1012/tcp

SSL/TLS: Not vulnerable to Heartbleed

port 1010/tcp

SSL/TLS: Not vulnerable to CCS Injection
port 1010/tcp

SSL/TLS: Not vulnerable to Ticketbleed
port 1010/tcp

SSL/TLS: Not vulnerable to ROBOT
port 1010/tcp

SSL/TLS: Not vulnerable to Secure Renegotiation
port 1010/tcp

SSL/TLS: Not vulnerable to CRIME
port 1010/tcp

SSL/TLS: Not vulnerable to POODLE
port 1010/tcp

SSL/TLS: Not vulnerable to SWEET32
port 1010/tcp

SSL/TLS: Not vulnerable to FREAK
port 1010/tcp

SSL/TLS: Not vulnerable to DROWN
port 1010/tcp

SSL/TLS: Not vulnerable to LOGJAM
port 1010/tcp

SSL/TLS: Not vulnerable to RC4
port 1010/tcp

Tested for SSL/TLS vulnerabilities
port 1010/tcp

SSL/TLS: Not vulnerable to Heartbleed
port 1011/tcp

SSL/TLS: Not vulnerable to CCS Injection
port 1011/tcp

SSL/TLS: Not vulnerable to Ticketbleed
port 1011/tcp

SSL/TLS: Not vulnerable to ROBOT
port 1011/tcp

SSL/TLS: Not vulnerable to Secure Renegotiation
port 1011/tcp

SSL/TLS: Not vulnerable to CRIME
port 1011/tcp

SSL/TLS: Not vulnerable to POODLE
port 1011/tcp

SSL/TLS: Not vulnerable to SWEET32
port 1011/tcp

SSL/TLS: Not vulnerable to FREAK
port 1011/tcp

SSL/TLS: Not vulnerable to DROWN
port 1011/tcp

SSL/TLS: Not vulnerable to LOGJAM
port 1011/tcp

SSL/TLS: Not vulnerable to BEAST
port 1011/tcp

SSL/TLS: Not vulnerable to RC4
port 1011/tcp

Tested for SSL/TLS vulnerabilities
port 1011/tcp

Scan coverage information

List of tests performed (73/73)

- ✓ 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...
- ✓ Checking if the certificate is trusted...
- ✓ Checking if the certificate is expired...
- ✓ Checking for Certificate Authority Issuer...
- ✓ Checking the certificate on port 1012...
- ✓ Checking if the certificate is trusted...
- ✓ Checking if the certificate is expired...
- ✓ Checking for Certificate Authority Issuer...
- ✓ Checking the certificate on port 1010...
- ✓ Checking if the certificate is trusted...

- ✓ Checking if the certificate is expired...
- ✓ Checking for Certificate Authority Issuer...
- ✓ Checking the certificate on port 1011...
- ✓ 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
- ✓ Scanning for HEARTBLEED on port 1012
- ✓ Scanning for CCS on port 1012
- ✓ Scanning for TICKETBLEED on port 1012
- ✓ Scanning for ROBOT on port 1012
- ✓ Scanning for SECURE_RENEGO on port 1012
- ✓ Scanning for CRIME_TLS on port 1012
- ✓ Scanning for POODLE_SSL on port 1012
- ✓ Scanning for SWEET32 on port 1012
- ✓ Scanning for FREAK on port 1012
- ✓ Scanning for DROWN on port 1012
- ✓ Scanning for LOGJAM on port 1012
- ✓ Scanning for BEAST on port 1012
- ✓ Scanning for RC4 on port 1012
- ✓ Tested for SSL/TLS vulnerabilities
- ✓ Scanning for HEARTBLEED on port 1010
- ✓ Scanning for CCS on port 1010
- ✓ Scanning for TICKETBLEED on port 1010
- ✓ Scanning for ROBOT on port 1010
- ✓ Scanning for SECURE_RENEGO on port 1010
- ✓ Scanning for CRIME_TLS on port 1010
- ✓ Scanning for POODLE_SSL on port 1010
- ✓ Scanning for SWEET32 on port 1010
- ✓ Scanning for FREAK on port 1010
- ✓ Scanning for DROWN on port 1010
- ✓ Scanning for LOGJAM on port 1010
- ✓ Scanning for BEAST on port 1010
- ✓ Scanning for RC4 on port 1010
- ✓ Tested for SSL/TLS vulnerabilities
- ✓ Scanning for HEARTBLEED on port 1011
- ✓ Scanning for CCS on port 1011
- ✓ Scanning for TICKETBLEED on port 1011
- ✓ Scanning for ROBOT on port 1011
- ✓ Scanning for SECURE_RENEGO on port 1011
- ✓ Scanning for CRIME_TLS on port 1011
- ✓ Scanning for POODLE_SSL on port 1011
- ✓ Scanning for SWEET32 on port 1011
- ✓ Scanning for FREAK on port 1011
- ✓ Scanning for DROWN on port 1011
- ✓ Scanning for LOGJAM on port 1011
- ✓ Scanning for BEAST on port 1011
- ✓ Scanning for RC4 on port 1011
- ✓ Tested for SSL/TLS vulnerabilities

Scan parameters

Target:	expired.badssl.com
Preset:	Deep
Scanning engines:	Certificate, Vulnerability
Ports to scan:	Top 1000 ports