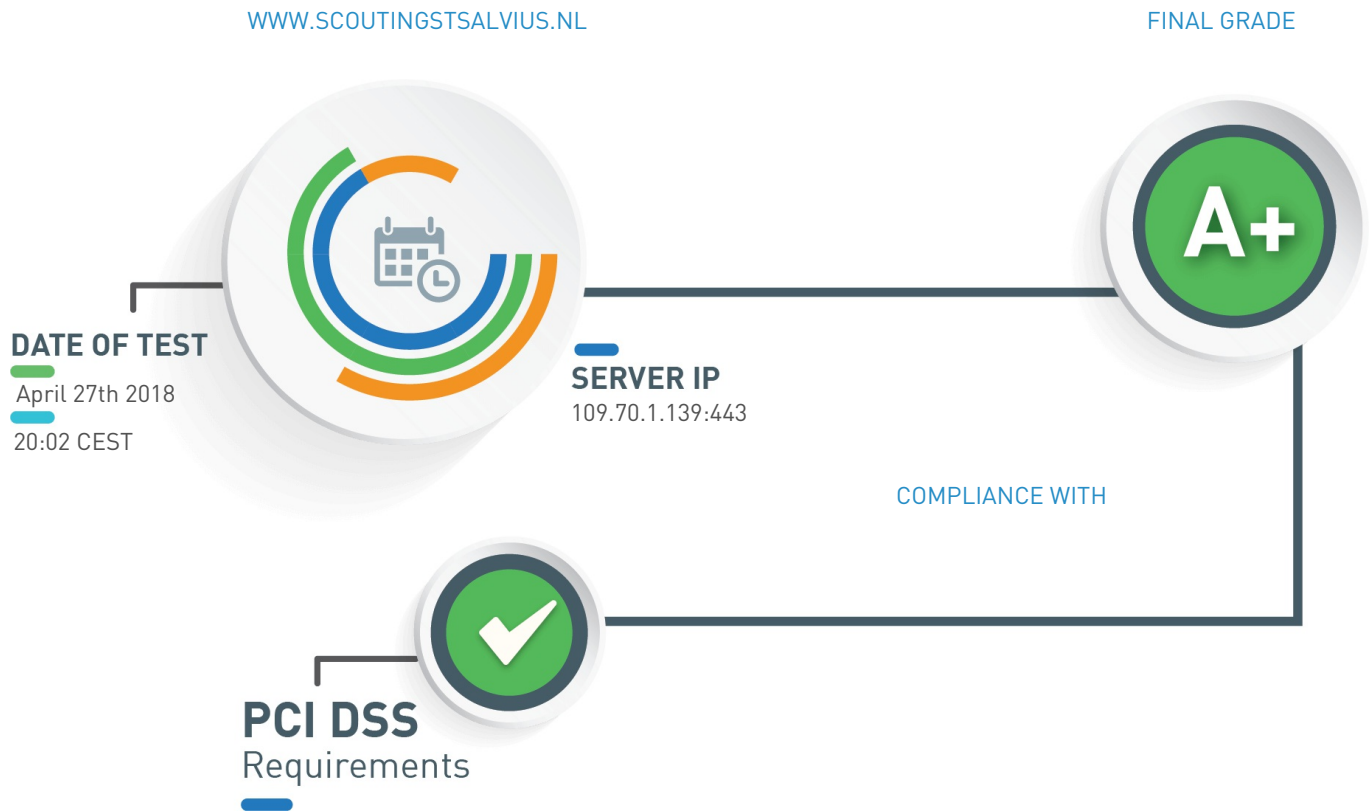


SSL/TLS Server Test of www.scoutingstsalvius.nl:443 (HTTPS)

Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.



Assessment Executive Summary

TEST HIGHLIGHTS

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website.	Information
The server configuration seems to be good, but is not entirely compliant with NIST guidelines and HIPAA guidance.	Information
The server prefers cipher suites supporting Perfect-Forward-Secrecy.	Good configuration
The server provides HTTP Strict Transport Security.	Good configuration

SSL Certificate Overview

RSA CERTIFICATE INFORMATION

Issuer	Let's Encrypt Authority X3
Trusted	Yes
Common Name	www.scoutingstsalvius...
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:scoutingstsalvius.nl, DNS:www.scoutingstsalvius.nl
Transparency	No
Validation Level	DV
CRL	No
OCSP	http://ocsp.int-x3.letsencrypt.org
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	March 2nd 2018, 21:00 CET
Valid To	May 31st 2018, 22:00 CEST

CERTIFICATE CHAIN

www.scoutingstsalvius.nl

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	8f846adea018a71e5fb5a64d5514c6a001ea91647b3bc199c9a29fd95cbac551
PIN	FokyY3uTs+H7WwZii8WJKJnPZkq9/UPF+c0Hxld9jAY=
Expires in	34 days

↑ Let's Encrypt Authority X3

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	e6e6a1bc74844586ea47eaa25b282758b987047fb7e2d0db782ee71691fa05d2
PIN	YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Expires in	1,055 days

↑ DST Root CA X3

Self-signed

Root CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha1WithRSAEncryption
SHA256	e756e3cf7da06f498ecd6abca535297f6adb087142855e030e88e3323611e66a

PIN	Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=
Expires in	1,252 days

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted.

Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Good configuration

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2

Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS.

Not vulnerable

CVE-2016-2107

The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).

Not vulnerable

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation.

Good configuration

ROBOT

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability.

Not vulnerable

HEARTBLEED

The server version of OpenSSL is not vulnerable to Heartbleed attack.

Not vulnerable

CVE-2014-0224

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).

Not vulnerable

Test For Compliance With HIPAA

Reference: HIPAA of 1996, Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3.

Good configuration

SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status.

Non-compliant with HIPAA guidance

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2

Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Good configuration

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

NO SUPPORT OF TLSV1.1

The support of TLSv1.1 is mandatory according to HIPAA guidance.

Non-compliant with HIPAA guidance

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 1 - Section 3

NIST Update to Current Use and Deprecation of TDEA abrogates 3DES authorized in the NIST guidelines.

Information

X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3.

Good configuration

SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status.

Non-compliant with NIST guidelines

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Good configuration

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Good configuration

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2

Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

NO SUPPORT OF TLSV1.1

The support of TLSv1.1 is mandatory according to NIST guidelines.

Non-compliant with NIST guidelines

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Test For Industry Best-Practices

DNSSCAA

This domain does not have a Certification Authority Authorization (CAA) record.

Information

CERTIFICATES DO NOT PROVIDE EV

The RSA certificate provided is NOT an Extended Validation (EV) certificate.

Information

SERVER HAS CIPHER PREFERENCE

The server enforces cipher suites preference.

Good configuration

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Good configuration

SERVER PREFERS CIPHER SUITES PROVIDING PFS

For TLS family of protocols, the server prefers cipher suite(s) providing Perfect Forward Secrecy (PFS).

Good configuration

ALWAYS-ON SSL

The HTTP version of the website redirects to the HTTPS version.

Good configuration

SERVER PROVIDES HSTS WITH LONG DURATION

The server provides HTTP Strict Transport Security for more than 6 months:

63072000 seconds

Good configuration

SERVER DOES NOT PROVIDE HPKP

The server does not enforce HTTP Public Key Pinning that helps preventing man-in-the-middle attacks.

Information

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation.

Good configuration

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration