


Summary of shop.tesla.com:443 (HTTPS) SSL Security Test

Provided "as is" without any warranty of any kind.

shop.tesla.com was tested 232 times during the last 12 months.

Your final score:

Date/Time:Sep 7th, 2024 19:49:06 GMT+5

Source IP/Port:23.223.216.107:443 

Type:HTTPS


A

B

C


F

A+




Compliance Test

COMPLIANT




Compliance Test

NO MAJOR ISSUES FOUND




Compliance Test

NO MAJOR ISSUES FOUND



Industry Best Practices

NO ISSUES FOUND



External Content Security

NOT FOUND

The server supports the most recent and secure TLS protocol version of TLS 1.3.

Good configuration

Discovered Subdomains

Hostname	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
tesla.com	HTTPS / 443	The RSA certificate is valid till Sep 30th 2024	Aug 5th, 2024 11:47:44 GMT+5	PCI DSS HIPAA	A+

Hostname	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
----------	---------------	----------------	-----------	-------------	-------

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	GeoTrust RSA CA 2018
Trusted	Yes
Common Name	*.tesla.com
Key Type/Size	RSA 2048 bits
Serial Number	14553443957376364800021074891932989029
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.tesla.com, DNS:tesla.com
Transparency	Yes
Validation Level	OV
CRL	http://cdp.geotrust.com/GeoTrustRSACA2018.crl
OCSP	http://status.geotrust.com
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	January 22, 2024 01:00 CET
Valid To	January 23, 2025 00:59 CET

CERTIFICATE CHAIN

<div><div>Root CA</div><div>DigiCert Global Root CA</div><div>Type/Size</div><div>RSA 2048 bits</div><div>Serial Number</div><div>1094471959895204037495183296379445434</div><div>Signature</div><div>sha1WithRSAEncryption</div><div>SHA256</div><div>4348a0e9444c78cb26... 257f8934a443c70161</div><div>PIN</div><div>r/mlkG3eEpVdm+u/ko... 1bk4TyHlByibiA5E=</div><div>Expires in</div><div>2,618 days</div><div>Comment</div><div>Self-signed</div></div>	<div><div>Intermediate CA</div><div>GeoTrust RSA CA 2018</div><div>Type/Size</div><div>RSA 2048 bits</div><div>Serial Number</div><div>7014754403668890451052340637799309683</div><div>Signature</div><div>sha256WithRSAEncryption</div><div>SHA256</div><div>8cc34e11c167045824... 112a859d661f8e2bc7</div><div>PIN</div><div>zUlraRNo+4JoAYA7RO... N4rIEbCpfCRQT6N6A=</div><div>Expires in</div><div>1,154 days</div><div>Comment</div><div>-</div></div>
<div><div>Server certificate</div><div>*.tesla.com</div><div>Type/Size</div><div>RSA 2048 bits</div><div>Serial Number</div><div>14553443957376364800021074891932989029</div></div>	

Signature	sha256WithRSAEncryption
SHA256	6521ba26b971fd8b2b... f765ff4cddd46e0fbd
PIN	9HuMDZkGYD6H1HTzWP... IV7aAH7PINcJd3W58=
Expires in	136 days
Comment	-

PCI DSS Compliance Test of cached

Reference: [PCI DSS 4.0](#), Requirement 4.2

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:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration
TLS_AES_128_CCM_8_SHA256	Good configuration
TLS_AES_128_CCM_SHA256	Good configuration

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
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:	
TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:	
P-256 (prime256v1) (256 bits)	Good configuration
X25519 (253 bits)	Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS.

Not vulnerable

GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE.

Not vulnerable

ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE.

Not vulnerable

SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE.

Not vulnerable

0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL.

Not vulnerable

CVE-2016-2107

The server is not vulnerable to 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 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 CCS Injection.

Not vulnerable

CVE-2021-3449

The server is not vulnerable to CVE-2021-3449 (OpenSSL Maliciously Crafted Renegotiation Vulnerability).

Not vulnerable

HIPAA and NIST Compliance Test

Reference: [HIPAA](#), Security Rule (Ref. [NIST SP 800-52](#): “Guidelines for the Selection and Use of TLS Implementations”)

X.509 CERTIFICATES ARE IN VERSION 3

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

Good configuration

SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status.

Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration
TLS_AES_128_CCM_8_SHA256	Good configuration
TLS_AES_128_CCM_SHA256	Good configuration

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
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

X25519 (253 bits)

Good configuration

SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET

The server does not support [Extended Master Secret \(EMS\)](#) extension for TLS versions ≤ 1.2 . EMS provides additional security to SSL sessions and prevents certain MitM attacks.

Non-compliant with NIST guidelines

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Industry Best Practices Test of cached

DNSCAA

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

Information

CERTIFICATES HAVE A VALIDITY PERIOD OF 398 DAYS OR LESS

All the server certificates provided have been validated for less than 398 days (13 months).

Good configuration

CERTIFICATES DO NOT PROVIDE EV

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

Information

TLS 1.3 SUPPORTED

The server supports TLS 1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Good configuration

TLS 1.3 EARLY DATA (0-RTT)

Server's TLS 1.3 Early Data (RFC 8446, page 17) is not enabled.

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

Good configuration

TLSv1.3

TLS_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

HSTS PRELOAD

This domain does not support HSTS Preload, which means it may not enforce HTTPS connections strictly and could be more vulnerable to security threats like protocol downgrade attacks.

Information

TLS_FALLBACK_SCSV

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

Good configuration

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

External Content Privacy and Security Analysis

No External Content appears to be loaded by the website.

Information

Need More? Upgrade to ImmuniWeb® AI Platform

Get remediation advice and ensure compliance with ImmuniWeb AI Platform:

Attack Surface
Management

Web Security
Scanning

Cybersecurity
Compliance

FREE DEMO

GET PRICING