📢 **MDN HTTP Observatory** is launched, and Mozilla Observatory is now deprecated. **Learn more.**

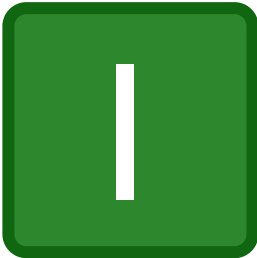HTTP Observatory

> **TLS Observatory**

SSH Observatory

Third-party Tests

Scan Summary

I

Host:	www.tesla.com (23.192.212.219)
Scan ID #:	59208831
End Time:	September 14, 2024 10:11 PM
Compat. Level:	Intermediate
Explainer:	189278767

Certificate

Common name:	*.tesla.com
Alternative Names:	*.tesla.com, tesla.com
First Observed:	2024-02-02 (certificate #189278767)
Valid From:	2024-01-22
Valid To:	2025-01-22
Key:	RSA 2048 bits
Issuer:	GeoTrust RSA CA 2018
Signature Algorithm:	SHA256WithRSA

Cipher Suites

Cipher	Code ⓘ	Size	AEAD ⓘ	PFS ⓘ	Protocols
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✔	✔	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✔	✔	TLS 1.2

Cipher	Code ⓘ	Size	AEAD ⓘ	PFS ⓘ	Protocols
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2

Miscellaneous

CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 4.4.2, Apple ATS 9, BingPreview Jan 2015, Chrome 30, Edge 12, Firefox 31.3.0 ESR, Googlebot Feb 2015, IE 11, Java 8b132, OpenSSL 1.0.1h, Opera 17, Safari 5, Yahoo Slurp Jun 2014, YandexBot Sep 2014
OCSP Stapling:	Yes

Suggestions

Looking for improved security and have a user base of only modern clients?

Take a look at the [Mozilla "Modern" TLS configuration](#)! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

[Want the detailed technical nitty-gritty?](#)

Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then hop on board:

<div align="center">

Teleport me to Mozilla's configuration generator!

</div>

Looking for improved security and have a user base of only modern clients?

Take a look at the [Mozilla "Modern" TLS configuration](#)! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

[Want the detailed technical nitty-gritty?](#)