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

- HTTP Observatory
- TLS Observatory
- SSH Observatory
- Third-party Tests

Scan Summary

Host:	ourshopee.com (172.66.43.59)
Scan ID #:	58181430
End Time:	July 7, 2024 3:19 PM
Compat. Level:	Non-compliant Please note that non-compliance simply means that the server's configuration is either more or less strict than a pre-defined Mozilla configuration level.
Explainer:	189559441

Certificate

Common name:	ourshopee.com
Alternative Names:	ourshopee.com, saudi.ourshopee.com, www.saudi.ourshopee.com, www.bahrain.ourshopee.com, www.kuwait.ourshopee.com, www.oman.ourshopee.com, www.qatar.ourshopee.com, *.ourshopee.com
First Observed:	2024-07-07 (certificate #189559441)
Valid From:	2024-06-28
Valid To:	2024-09-26
Key:	ECDSA 256 bits, curve P-256
Issuer:	WE1
Signature Algorithm:	ECDSAWithSHA256

Cipher Suites

Cipher	Code ()	Size	AEAD ()	PFS ()	Protocols
ECDHE-ECDSA-CHACHA20-POLY1305-OLD	`0xCC 0x14`	256 bits	✓	✓	TLS 1.2
ECDHE-ECDSA-AES128-GCM-SHA256	`0x0C 0x2B`	256 bits	✓	✓	TLS 1.2
ECDHE-ECDSA-AES128-SHA	`0x0C 0x09`	256 bits	✗	✓	TLS 1.2
ECDHE-ECDSA-AES256-GCM-SHA384	`0x0C 0x2C`	256 bits	✓	✓	TLS 1.2
ECDHE-ECDSA-AES256-SHA	`0x0C 0x0A`	256 bits	✗	✓	TLS 1.2
ECDHE-ECDSA-AES128-SHA256	`0x0C 0x23`	256 bits	✗	✓	TLS 1.2
ECDHE-ECDSA-AES256-SHA384	`0x0C 0x24`	256 bits	✗	✓	TLS 1.2
ECDHE-RSA-CHACHA20-POLY1305-OLD	`0xCC 0x13`	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	`0x0C 0x2F`	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-SHA	`0x0C 0x13`	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-GCM-SHA256	`0x00 0x9C`	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA	`0x00 0x2F`	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES256-GCM-SHA384	`0x0C 0x30`	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	`0x0C 0x14`	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-GCM-SHA384	`0x00 0x9D`	2048 bits	✓	✗	TLS 1.2
RSA-AES256-SHA	`0x00 0x35`	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES128-SHA256	`0x0C 0x27`	2048 bits	✗	✓	TLS 1.2
RSA-AES128-SHA256	`0x00 0x3C`	2048 bits	✗	✗	TLS 1.2
ECDHE-RSA-AES256-SHA384	`0x0C 0x28`	2048 bits	✗	✓	TLS 1.2
RSA-AES256-SHA256	`0x00 0x3D`	2048 bits	✗	✗	TLS 1.2
RSA-DES-CBC3-SHA	`0x00 0x0A`	2048 bits	✗	✗	TLS 1.0

Miscellaneous

CAA Record:	Yes, on ourshopee.com
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 2.3.7, Apple ATS 9, Baidu Jan 2015, BingBot Dec 2013, BingPreview Dec 2013, Chrome 27, Edge 12, Firefox 21, Googlebot Oct 2013, IE 7, Java 6u45, OpenSSL 0.9.8y, Opera 12.15, Safari 5, Tor 17.0.9, Yahoo Slurp Oct 2013, YandexBot May 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?

Still want secure website, but need compatibility with those older clients?

No problem! The Mozilla “Intermediate” TLS configuration may be just right for you! It provides the similar level of security to the “Modern” configuration when used with current clients, but still supports older versions of web browsers and tools.

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:

Teleport me to Mozilla's configuration generator!