

🔊 MDN HTTP Observatory is launched, and Mozilla Observatory is now deprecated. [Learn more.](#)

<a href="#">HTTP Observatory</a>
<a href="#">TLS Observatory</a>
<a href="#">SSH Observatory</a>
<a href="#">Third-party Tests</a>

Scan Summary

Host:	vendasta.com (34.107.155.167)
Scan ID #:	58181408
End Time:	July 7, 2024 3:14 PM
Compat. Level:	Intermediate
Explainer:	<a href="#">189559439</a>

Certificate

Common name:	vendasta.com
Alternative Names:	vendasta.com
First Observed:	2024-07-07 (certificate # <a href="#">189559439</a> )
Valid From:	2024-06-12
Valid To:	2024-09-10
Key:	RSA 2048 bits
Issuer:	R11
Signature Algorithm:	SHA256WithRSA

Cipher Suites					
Cipher	Code	Size	AEAD	PFS	Protocols
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0

Cipher	Code	Size	AEAD	PFS	Protocols
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2
RSA-AES256-GCM-SHA384	0x00 0x9D	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-DES-CBC3-SHA	0x00 0x0A	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0

Miscellaneous	
CAA Record:	No
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:	No

Suggestions	
Looking for improved security and have a user base of only modern clients?	
Take a look at the <a href="#">Mozilla “Modern” TLS configuration</a> ! 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.	
<a href="#">Want the detailed technical nitty-gritty?</a>	
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>Teleport me to Mozilla's configuration generator!</div>	