Scan Summary

Host:	qasvus.wixsite.com (199.15.163.145)
Scan ID #:	51787271
End Time:	October 20, 2022 6:59 PM
Compatibility 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.
Certificate Explainer:	188827235

Certificate Information

Common name:	*.wix.com
Alternative Names:	*.wix.com, *.editorx.com, *.wixsite.com, editorx.com, wix.com, wixsite.com
First Observed:	2022-06-03 (certificate #188827235)
Valid From:	2022-05-16
Valid To:	2022-11-12
Key:	RSA 2048 bits
Issuer:	Sectigo RSA Domain Validation Secure Server CA
Signature Algorithm:	SHA256WithRSA

Cipher Suites

Cipher Suite	Code ()	Key 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
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2
RSA-AES128-SHA256	0x00 0x3C	2048 bits	✗	✗	TLS 1.2
RSA-AES256-GCM-SHA384	0x00 0x9D	2048 bits	✓	✗	TLS 1.2
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2
RSA-AES256-SHA256	0x00 0x3D	2048 bits	✗	✗	TLS 1.2
RSA-CAMELLIA128-SHA	0x00 0x41	2048 bits	✗	✗	TLS 1.2
RSA-CAMELLIA256-SHA	0x00 0x84	2048 bits	✗	✗	TLS 1.2
DHE-RSA-AES128-GCM-SHA256	0x00 0x9E	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES128-SHA	0x00 0x33	2048 bits	✗	✓	TLS 1.2
DHE-RSA-AES128-SHA256	0x00 0x67	2048 bits	✗	✓	TLS 1.2
DHE-RSA-AES256-GCM-SHA384	0x00 0x9F	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES256-SHA	0x00 0x39	2048 bits	✗	✓	TLS 1.2
DHE-RSA-AES256-SHA256	0x00 0x6B	2048 bits	✗	✓	TLS 1.2
DHE-RSA-CAMELLIA128-SHA	0x00 0x45	2048 bits	✗	✓	TLS 1.2
DHE-RSA-CAMELLIA256-SHA	0x00 0x88	2048 bits	✗	✓	TLS 1.2

Miscellaneous Information

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:	No

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!