QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.lvh.io > 2400:cb00:2048:1:0:0:6812:2239

SSL Report: www.lvh.io (2400:cb00:2048:1:0:0:6812:2239)

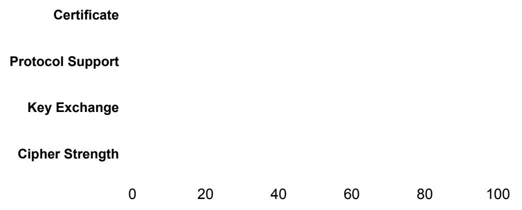
Assessed on: Wed, 25 May 2016 20:52:49 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	sni103656.cloudflaressl.com Fingerprint SHA1: d6852d1f56ef14f6beaaab88dce7d8c1b6b47743 Pin SHA256: +R9iIALeimuDp0N49HQO/IAzPXLnzUJnYmriw2CHlJ0=
Common names	sni103656.cloudflaressl.com
Alternative names	sni103656.cloudflaressl.com *.asiatesoulagedirect.eu *.casamestica.com.br *.crypto101.io *.lvh.cc *.lvh.io *.morinvilleflowers.ca *.wpfreshstart.com *.zz380.com asiatesoulagedirect.eu casamestica.com.br crypto101.io lvh.cc lvh.io morinvilleflowers.ca wpfreshstart.com zz380.com
Valid from	Sun, 08 May 2016 00:00:00 UTC
Valid until	Sun, 13 Nov 2016 23:59:59 UTC (expires in 5 months and 19 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	COMODO ECC Domain Validation Secure Server CA 2 AIA: http://crt.comodoca4.com/COMODOECCDomainValidationSecureServerCA2.crt
Signature algorithm	SHA256withECDSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca4.com/COMODOECCDomainValidationSecureServerCA2.crl OCSP: http://ocsp.comodoca4.com
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	3 (3175 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	COMODO ECC Domain Validation Secure Server CA 2 Fingerprint SHA1: 75cfd9bc5cefa104ecc1082d77e63392ccba5291 Pin SHA256: x9SZw6TwIqfmvrLZ/kz1o0Ossjmn728BnBKpUFqGNVM=
Valid until	Mon, 24 Sep 2029 23:59:59 UTC (expires in 13 years and 3 months)
Key	EC 256 bits
Issuer	COMODO ECC Certification Authority
Signature algorithm	SHA384withECDSA

#3

Subject	COMODO ECC Certification Authority Fingerprint SHA1: ae223cbf20191b40d7ffb4ea5701b65fdc68a1ca Pin SHA256: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 4 years)
Key	EC 384 bits
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	sni103656.cloudflaressl.com Fingerprint SHA1: d6852d1f56ef14f6beaaab88dce7d8c1b6b47743 Pin SHA256: +R9iIALeimuDp0N49HQO/IAzPXLnzUJnYmriw2CHlJ0= EC 256 bits / SHA256withECDSA
2	Sent by server	COMODO ECC Domain Validation Secure Server CA 2 Fingerprint SHA1: 75cfd9bc5cefa104ecc1082d77e63392ccba5291 Pin SHA256: x9SZw6TwIqfmvrLZ/kz1o0Ossjmn728BnBKpUFqGNVM= EC 256 bits / SHA384withECDSA
3	In trust store	COMODO ECC Certification Authority Self-signed Fingerprint SHA1: 9f744e9f2b4dbaec0f312c50b6563b8e2d93c311 Pin SHA256: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU= EC 384 bits / SHA384withECDSA

Path #2: Trusted

1	Sent by server	sni103656.cloudflaressl.com Fingerprint SHA1: d6852d1f56ef14f6beaaab88dce7d8c1b6b47743 Pin SHA256: +R9iIALeimuDp0N49HQO/IAzPXLnzUJnYmriw2CHlJ0= EC 256 bits / SHA256withECDSA
2	Sent by server	COMODO ECC Domain Validation Secure Server CA 2 Fingerprint SHA1: 75cfd9bc5cefa104ecc1082d77e63392ccba5291 Pin SHA256: x9SZw6TwIqfmvrLZ/kz1o0Ossjmn728BnBKpUFqGNVM= EC 256 bits / SHA384withECDSA
3	Sent by server	COMODO ECC Certification Authority Fingerprint SHA1: ae223cbf20191b40d7ffb4ea5701b65fdc68a1ca Pin SHA256: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU= EC 384 bits / SHA384withRSA
4	In trust store	AddTrust External CA Root Self-signed Fingerprint SHA1: 02faf3e291435468607857694df5e45b68851868 Pin SHA256: lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	112
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256[P]
OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256[P]

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Handshake Simulation

Android 2.3.7 No SNI [2]	Server sent fatal alert: internal_error				
Android 4.0.4	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.1.1	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.2.2	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.3	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	EC 256 (SHA256)	TLS 1.2	OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
Baidu Jan 2015	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 48 / OS X R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 42 / OS X R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 44 / OS X R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 6 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure				
IE 7 / Vista	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: internal_error				
IE 8-10 / Win 7 R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 10 / Win Phone 8.0	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 6u45 No SNI [2]	Server sent fatal alert: internal_error				
Java 7u25	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u31	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8y	Server sent fatal alert: handshake_failure				
OpenSSL 1.0.1l R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.2e R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 5.1.9 / OS X 10.6.8	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 7 / OS X 10.9 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 8 / iOS 8.4 R	EC 256 (SHA256)	TLS 1.2 > spdy/3.1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 8 / OS X 10.10 R	EC 256 (SHA256)	TLS 1.2 > spdy/3.1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

Handshake Simulation

Apple ATS 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: `0xc009`
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes
NPN	Yes h2 spdy/3.1 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=15552000; preload
HSTS Preloading	**Not in: Chrome Edge Firefox IE Tor**
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	No

Miscellaneous

Test date	Wed, 25 May 2016 20:48:49 UTC
Test duration	58.425 seconds
HTTP status code	200
HTTP server signature	cloudflare-nginx
Server hostname	-

SSL Report v1.22.37

Terms and Conditions