SSL Report: libreduca.com (162.243.224.177)

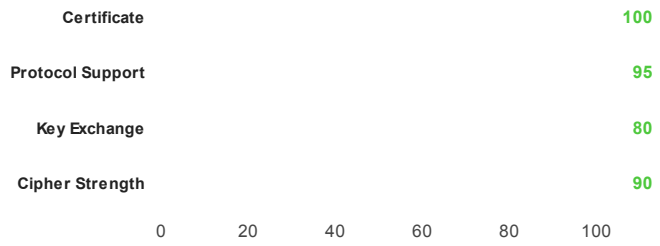
Assessed on: Thu Mar 27 16:50:36 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Authentication

Server Key and Certificate #1

Common names	*.libreduca.com
Alternative names	*.libreduca.com libreduca.com
Prefix handling	Both (with and without WWW)
Valid from	Mon Feb 10 00:00:00 UTC 2014
Valid until	Tue Feb 10 23:59:59 UTC 2015 (expires in 10 months and 20 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	PositiveSSL CA 2
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (2545 bytes)
Chain issues	None

#2

Subject	PositiveSSL CA 2 SHA1: 94807b1c788dd2fcbe19c8481ce41cfab8a4c17f
Valid until	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 2 months)
Key	RSA 2048 bits
Issuer	AddTrust External CA Root

Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	*.libreduca.com SHA1: b2bc65180763437e1c057970ec11f5d265d585c1 RSA 2048 bits / SHA1withRSA
2	Sent by server	PositiveSSL CA 2 SHA1: 94807b1c788dd2fcbe19c8481ce41cfab8a4c17f RSA 2048 bits / SHA1withRSA
3	In trust store	AddTrust External CA Root SHA1: 02faf3e291435468607857694df5e45b68851868 RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	*.libreduca.com SHA1: b2bc65180763437e1c057970ec11f5d265d585c1 RSA 2048 bits / SHA1withRSA
2	Sent by server	PositiveSSL CA 2 SHA1: 94807b1c788dd2fcbe19c8481ce41cfab8a4c17f RSA 2048 bits / SHA1withRSA
3	Extra dow nload	AddTrust External CA Root SHA1: 53845e9fd070b7aa36976f536ff1441c578c63d2 RSA 2048 bits / SHA1withRSA
4	In trust store	UTN - DATACorp SGC SHA1: 58119f0e128287ea50fdd987456f4f78dcfad6d4 RSA 2048 bits / SHA1withRSA

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, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) FS		128
TLS_RSA_WITH_RC4_128_SHA (0x5)		128

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 33 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Firefox 27 / Win 8 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
YandexBot 3.0 No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]

(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 tend to 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

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) TLS 1.0: 0xc011
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
Next Protocol Negotiation	Yes http/1.1

Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Thu Mar 27 16:49:39 UTC 2014
Test duration	57.332 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	libreduca.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.9.2

Copyright © 2009-2014 Qualys, Inc. All Rights Reserved.

Terms and Conditions