You are here: Home > Projects > SSL Server Test > libreduca.com

SSL Report: libreduca.com (192.81.217.8)

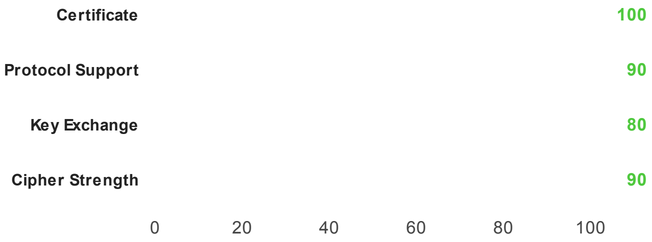
Assessed on: Fri Dec 13 13:39:14 UTC 2013 | Clear cache

Scan Another »

Summary

Overall Rating

A



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

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 Jan 14 00:00:00 UTC 2013
Valid until	Wed Feb 12 23:59:59 UTC 2014 (expires in 2 months and 1 day)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	EssentialSSL CA
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	4 (4992 bytes)
Chain issues	None

#2

Subject	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7
Valid until	Tue Dec 31 23:59:59 UTC 2019 (expires in 6 years)
Key	RSA 2048 bits
Issuer	COMODO Certification Authority
Signature algorithm	SHA1withRSA

#3

Subject	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e
Valid until	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 5 months)
Key	RSA 2048 bits
Issuer	UTN - DATACorp SGC
Signature algorithm	SHA1withRSA

#4

Subject	UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63
Valid until	Sat May 30 10:48:38 UTC 2020 (expires in 6 years and 5 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: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	In trust store	COMODO Certification Authority SHA1: 6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	*.libreduca.com SHA1: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	In trust store	UTN - DATACorp SGC SHA1: 58119f0e128287ea50fdd987456f4f78dcfad6d4 RSA 2048 bits / SHA1withRSA

Path #3: Trusted

1	Sent by server	*.libreduca.com SHA1: 8ecea8cb7ae8a701bb14e0bdb89276536a6c2ef6 RSA 2048 bits / SHA1withRSA
2	Sent by server	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7 RSA 2048 bits / SHA1withRSA
3	Sent by server	COMODO Certification Authority SHA1: 4e154acb683efd5578001432b92afe896812b85e RSA 2048 bits / SHA1withRSA
4	Sent by server	UTN - DATACorp SGC SHA1: 9e99817d12280c9677674430492eda1dce2e4c63 RSA 2048 bits / SHA1withRSA
5	In trust store	AddTrust External CA Root SHA1: 02faf3e291435468607857694df5e45b68851868 RSA 2048 bits / SHA1withRSA

Configuration

Protocols

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

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

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

BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 31 / Win 7	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 17.0.7 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 24 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Googlebot Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
IE 8-10 / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
IE 11 / Win 7	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
IE 11 / Win 8.1	Protocol or cipher suite mismatch		Fail[3]
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_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) 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_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 6 / iOS 6.0.1	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Safari 6.0.4 / OS X 10.8.4	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 7 / OS X 10.9	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) FS	256
Tor 17.0.9 / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256

(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.

Protocol Details

Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x39, TLS 1.0: 0x39
TLS compression	No
RC4	Yes NOT DESIRABLE (more info)
Forward Secrecy	With some browsers (more info)
Next Protocol Negotiation	No
Session resumption	Yes
Session tickets	Yes
OCSP stapling	No
Strict Transport Security	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	Fri Dec 13 13:38:31 UTC 2013
Test duration	42.72 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.22 (Ubuntu)
Server hostname	libreduca.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.6.30