

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > libreunir.com

## SSL Report: libreunir.com (198.199.69.203)

Assessed on: Fri Sep 13 18:21:15 UTC 2013 | [Clear cache](#)

[Scan Another >>](#)

### Summary

#### Overall Rating



Certificate	100
Protocol Support	90
Key Exchange	80
Cipher Strength	90

0 20 40 60 80 100

Documentation: [SSL/TLS Deployment Best Practices](#) and [SSL Server Rating Guide](#).

This server supports [Forward Secrecy](#) with modern browsers.

### Authentication



#### Server Key and Certificate #1

Common names	libreunir.com
Alternative names	libreunir.com www.libreunir.com
Prefix handling	Both (with and without WWW)
Valid from	Sun Apr 07 00:00:00 UTC 2013
Valid until	Mon Apr 07 23:59:59 UTC 2014 (expires in 6 months and 26 days)
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	3 (3790 bytes)
Chain issues	None

#### #2

Subject	EssentialSSL CA SHA1: 73820a20f8f47a457cd0b54cc4e4e31cefa5c1e7
Valid until	Tue Dec 31 23:59:59 UTC 2019 (expires in 6 years and 3 months)
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 8 months)
Key	RSA 2048 bits
Issuer	UTN - DATACorp SGC
Signature algorithm	SHA1withRSA



### Certification Paths

#### Path #1: Trusted

1	Sent by server	libreunir.com SHA1: 3037b39dc975de07e43a2b61ecd873d4693d932d 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	libreunir.com SHA1: 3037b39dc975de07e43a2b61ecd873d4693d932d 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: 58119f0e128287ea50 added 987456f4f78dcfad6d4 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_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

<a href="#">Chrome 29 / Win 7</a>	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
<a href="#">Firefox 10.0.12 ESR / Win 7</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">Firefox 17.0.7 ESR / Win 7</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">Firefox 21 / Fedora 19</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Firefox 22 / Win 7</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">IE 6 / XP</a> No FS *	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 7 / Vista</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
<a href="#">IE 8 / XP</a> No FS *	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS	128
<a href="#">IE 8-10 / Win 7</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
<a href="#">IE 11 / Win 8.1</a>	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
<a href="#">Java 6u45</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
<a href="#">Java 7u25</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">OpenSSL 0.9.8y</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">OpenSSL 1.0.1e</a>	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
<a href="#">Opera 12.15 / Win 7</a>	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
<a href="#">Opera 15 / Win 7</a>	TLS 1.1	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">Safari 6 / iOS 6.0.1</a>	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
<a href="#">Safari 6.0.4 / OS X 10.8.4</a>	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS	128
<a href="#">Safari 7 / OS X 10.9</a>	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256

\* Browsers that do not support Forward Secrecy are excluded when determining support for it.



### Protocol Details

<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	No longer rated; considered sufficiently mitigated client-side ( <a href="#">more info</a> )
TLS compression	No
<b>RC4</b>	<b>Yes NOT DESIRABLE</b> ( <a href="#">more info</a> )
<b>Forward Secrecy</b>	<b>Yes</b> ( <a href="#">more info</a> )
Next Protocol Negotiation	Yes <a href="#">http/1.1</a>
Session resumption	Yes
Session tickets	Yes
OCSP stapling	No
<b>Strict Transport Security</b>	<b>Yes</b> 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 Sep 13 18:20:30 UTC 2013
Test duration	44.556 seconds
HTTP status code	200
HTTP server signature	nginx/1.4.1 + Phusion Passenger 4.0.10
Server hostname	libreunir.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.5.5