QUALYS SSL LABS

Home Projects Qualys.com Co

You are here: Home > Projects > SSL Server Test > email.cacert.org

SSL Report: email.cacert.org (213.154.225.228)

Assessed on: Sun Jan 25 09:25:03 PST 2015 | Clear cache

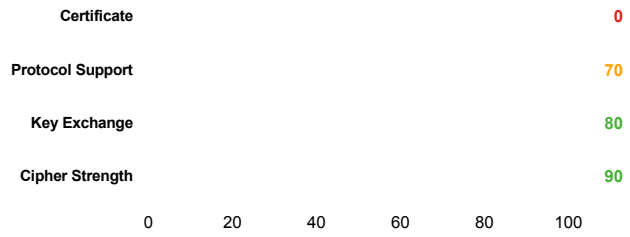
Scan Anotl

Summary

Overall Rating

T

If trust issues are ignored: B



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

This server's certificate is not trusted, see below for details.

This server does not mitigate the CRIME attack. Grade capped to B.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

There is no support for secure renegotiation. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Common names	community.cacert.org
Alternative names	community.cacert.org nocert.community.cacert.org cert.community.cacert.org email.cacert.org nocert.email.cacert.org cert.email.cacert.org
Prefix handling	Not required for subdomains
Valid from	Tue Apr 08 14:21:02 PDT 2014
Valid until	Thu Apr 07 14:21:02 PDT 2016 (expires in 1 year and 2 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	CA Cert Signing Authority
Signature algorithm	SHA512withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Unchecked (only trusted certificates can be checked)
Trusted	No **NOT TRUSTED** (Why?)

Additional Certificates (if supplied)

Certificates provided	2 (3811 bytes)
Chain issues	**Contains anchor**

#2

Subject	CA Cert Signing Authority Not in trust store Fingerprint: 135cec36f49cb8e93b1ab270cd80884676ce8f33
Valid until	Tue Mar 29 05:29:49 PDT 2033 (expires in 18 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	CA Cert Signing Authority Self-signed
Signature algorithm	MD5withRSA Weak, but no impact on root certificate

Certification Paths

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server	community.cacert.org Fingerprint: 9b8e0a6896e5c8e6e68ed810313f7c2ca84ee13f RSA 4096 bits (e 65537) / SHA512withRSA
2	Sent by server Not in trust store	CA Cert Signing Authority Self-signed Fingerprint: 135cec36f49cb8e93b1ab270cd80884676ce8f33 RSA 4096 bits (e 65537) / MD5withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

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

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	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_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.4.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
BingPreview Jun 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 39 / OS X R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Firefox 31.3.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256

Handshake Simulation

Firefox 34 / OS X R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Googlebot Jun 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE 8 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE 11 / Win 10 Preview R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
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
Java 8b132	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 1.0.1h	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) 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 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 8 / iOS 8.0 Beta R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Yahoo Slurp Jun 2014 No SNI [2]	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
YandexBot Sep 2014	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.

(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	**Not supported ACTION NEEDED** (more info)
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x39
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Unknown (requires support for at least two protocols)
TLS compression	**Yes INSECURE** (more info)
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**With some browsers** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No

Protocol Details	
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	**TLS 2.98**
SSL 2 handshake compatibility	Yes

Miscellaneous	
Test date	Sun Jan 25 09:24:07 PST 2015
Test duration	55.184 seconds
HTTP status code	302
HTTP forwarding	https://community.cacert.org
HTTP server signature	Apache
Server hostname	email.cacert.org

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall int categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificate our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maint own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, suc sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust tha self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded i browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the s We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot you may be able to provide us with information that might help us determine the root cause.

SSL Report v1.12.8