QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > gmail.com > 74.125.239.53

SSL Report: gmail.com (74.125.239.53)

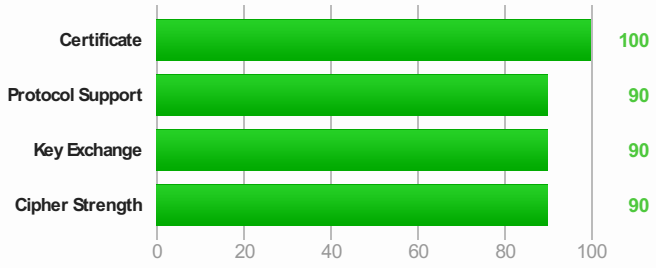
Assessed on: Mon Jun 23 06:26:19 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A



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

This site works only in browsers with SNI support.

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication

Server Key and Certificate #1

Common names	www.gmail.com
Alternative names	www.gmail.com
Prefix handling	Not valid for "gmail.com" CONFUSING
Valid from	Wed Jun 04 09:24:23 UTC 2014
Valid until	Tue Sep 02 00:00:00 UTC 2014 (expires in 2 months and 10 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	Google Internet Authority G2
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (3073 bytes)
Chain issues	None

#2

Subject	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24
Valid until	Sat Apr 04 15:15:55 UTC 2015 (expires in 9 months and 15 days)

Key	RSA 2048 bits
Issuer	GeoTrust Global CA
Signature algorithm	SHA1withRSA

#3

Subject	GeoTrust Global CA SHA1: 7359755c6df9a0abc3060bce369564c8ec4542a3
Valid until	Tue Aug 21 04:00:00 UTC 2018 (expires in 4 years and 1 month)
Key	RSA 2048 bits
Issuer	Equifax / Equifax Secure Certificate Authority
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	www.gmail.com SHA1: d338b65dc27ae61a2dfaca502fa544f17b4104aa RSA 2048 bits / SHA1withRSA
2	Sent by server	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24 RSA 2048 bits / SHA1withRSA
3	In trust store	GeoTrust Global CA SHA1: de28f4a4ffe5b92fa3c503d1a349a7f9962a8212 RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	www.gmail.com SHA1: d338b65dc27ae61a2dfaca502fa544f17b4104aa RSA 2048 bits / SHA1withRSA
2	Sent by server	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24 RSA 2048 bits / SHA1withRSA
3	Sent by server	GeoTrust Global CA SHA1: 7359755c6df9a0abc3060bce369564c8ec4542a3 RSA 2048 bits / SHA1withRSA
4	In trust store	Equifax / Equifax Secure Certificate Authority SHA1: d23209ad23d314232174e40d7f9d62139786633a RSA 1024 bits / SHA1withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Configuration

Protocols

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

(2) This site requires support for virtual SSL hosting, but SSL 2.0 and SSL 3.0 do not support this feature.

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

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) 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_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	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_128_GCM_SHA256 (0xc02f) FS	128
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Chrome 34 / OS X 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 29 / OS X 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]	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
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_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	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_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
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_128_CBC_SHA (0xc013) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
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_128_CBC_SHA (0xc013) FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128

(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.

(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) SSL 3: 0xc011, TLS 1.0: 0xc011
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation	Yes spdy/3.1 spdy/3 http/1.1
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Mon Jun 23 06:24:47 UTC 2014
Test duration	46.141 seconds
HTTP status code	301
HTTP forwarding	https://mail.google.com
HTTP server signature	sffe
Server hostname	nuq04s19-in-f21.1e100.net
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11