QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > mail.yahoo.com > 98.136.189.41

SSL Report: mail.yahoo.com (98.136.189.41)

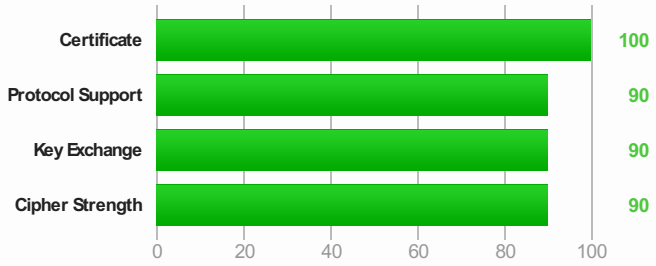
Assessed on: Mon Jun 23 10:00:00 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A



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

This server 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	*.login.yahoo.com
Alternative names	*.login.yahoo.com *.mail.yahoo.com *.edit.yahoo.com *.login.yahoo.net login.yahoo.com mail.yahoo.com mail.yahoo-inc.com fb.member.yahoo.com login.korea.yahoo.com api.reg.yahoo.com edit.yahoo.com watchlist.yahoo.com edit.india.yahoo.com edit.korea.yahoo.com edit.europe.yahoo.com edit.singapore.yahoo.com edit.tpe.yahoo.com legalredirect.yahoo.com me.yahoo.com open.login.yahooapis.com subscribe.yahoo.com edit.secure.yahoo.com edit.client.yahoo.com bt.edit.client.yahoo.com verizon.edit.client.yahoo.com na.edit.client.yahoo.com au.api.reg.yahoo.com au.reg.yahoo.com profile.yahoo.com static.profile.yahoo.com openid.yahoo.com
Prefix handling	Not required for subdomains
Prefix handling	Both (with and without WWW)
Valid from	Tue Apr 08 00:00:00 UTC 2014
Valid until	Thu Apr 09 23:59:59 UTC 2015 (expires in 9 months and 20 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	VeriSign Class 3 Secure Server CA - G3
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (4761 bytes)
Chain issues	None

#2

Subject	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476
Valid until	Fri Feb 07 23:59:59 UTC 2020 (expires in 5 years and 7 months)
Key	RSA 2048 bits
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA1withRSA

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27
Valid until	Sun Nov 07 23:59:59 UTC 2021 (expires in 7 years and 4 months)
Key	RSA 2048 bits
Issuer	VeriSign / Class 3 Public Primary Certification Authority
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA 2048 bits / SHA1withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 RSA 2048 bits / SHA1withRSA

Path #2: Not trusted (Algorithm constraints check failed: MD2withRSA)

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA 2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA 2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: 742c3192e607e424eb4549542be1bbc53e6174e2 RSA 1024 bits / MD2withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Path #3: Trusted

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA 2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA 2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: a1db6393916f17e4185509400415c70240b0ae6b 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	Yes
SSL 2	No

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_AES_256_GCM_SHA384 (0xc030) 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_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) 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_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

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_SHA256 (0xc027) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) 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_SHA256 (0xc027) 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_SHA256 (0xc027) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) 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_SHA256 (0xc027) 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)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation	Yes http/1.1 http/1.0
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 09:57:48 UTC 2014
Test duration	79.73 seconds
HTTP status code	200
HTTP server signature	ATS
Server hostname	ats1.member.vip.gq1.yahoo.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11