QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > hotmail.com > 157.55.152.112

SSL Report: hotmail.com (157.55.152.112)

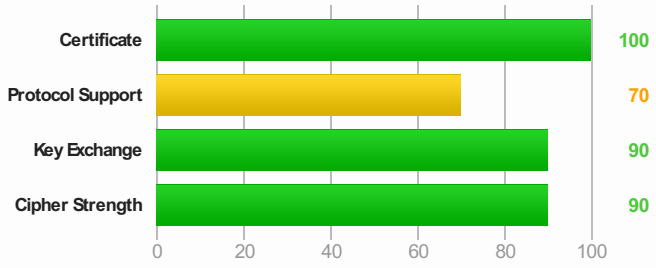
Assessed on: Sun Jun 22 15:28:01 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

B



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

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

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

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	mail.live.com
Alternative names	mail.live.com m.mail.live.com contacts.live.com hotmail.co.jp hotmail.co.uk hotmail.com hotmail.live.com hotmail.msn.com people.live.com www.hotmail.com www.hotmail.msn.com www.mail.live.com home.live.com www.live.com dvt.mail.live.com snt002.afx.ms snt002.mail.live.com snt110.afx.ms snt110.mail.live.com snt111.afx.ms snt111.mail.live.com snt112.afx.ms snt112.mail.live.com snt113.afx.ms snt113.mail.live.com snt114.afx.ms snt114.mail.live.com snt115.afx.ms snt115.mail.live.com snt116.afx.ms snt116.mail.live.com snt117.afx.ms snt117.mail.live.com snt118.afx.ms snt118.mail.live.com snt120.afx.ms snt120.mail.live.com snt121.afx.ms snt121.mail.live.com snt122.afx.ms snt122.mail.live.com snt123.afx.ms snt123.mail.live.com snt124.afx.ms snt124.mail.live.com snt125.afx.ms snt125.mail.live.com snt126.afx.ms snt126.mail.live.com snt127.afx.ms snt127.mail.live.com snt128.afx.ms snt128.mail.live.com snt129.afx.ms snt129.mail.live.com snt130.afx.ms snt130.mail.live.com snt131.afx.ms snt131.mail.live.com snt132.afx.ms snt132.mail.live.com snt133.afx.ms snt133.mail.live.com snt134.afx.ms snt134.mail.live.com snt135.afx.ms snt135.mail.live.com snt136.afx.ms snt136.mail.live.com snt137.afx.ms snt137.mail.live.com snt138.afx.ms snt138.mail.live.com snt139.afx.ms snt139.mail.live.com snt140.afx.ms snt140.mail.live.com snt141.afx.ms snt141.mail.live.com snt142.afx.ms snt142.mail.live.com snt143.afx.ms snt143.mail.live.com snt144.afx.ms snt144.mail.live.com snt145.afx.ms snt145.mail.live.com snt146.afx.ms snt146.mail.live.com snt147.afx.ms snt147.mail.live.com snt148.afx.ms snt148.mail.live.com
Prefix handling	Both (with and without WWW)
Valid from	Tue May 21 00:00:00 UTC 2013

Valid until	Fri May 22 23:59:59 UTC 2015 (expires in 10 months and 33 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	VeriSign Class 3 Extended Validation SSL SGC CA
Signature algorithm	SHA1withRSA
Extended Validation	**Yes**
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	3 (6062 bytes)
Chain issues	None

#2

Subject	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab
Valid until	Mon Nov 07 23:59:59 UTC 2016 (expires in 2 years and 4 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	mail.live.com SHA1: 9872bc7b7244dfef5e019acf73bad250ecaf9f80 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab 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	mail.live.com SHA1: 9872bc7b7244dfef5e019acf73bad250ecaf9f80 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab 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	mail.live.com SHA1: 9872bc7b7244dfef5e019acf73bad250ecaf9f80 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab 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	No
TLS 1.1	No
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_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 384 bits (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH 384 bits (eq. 7680 bits RSA) FS	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Android 4.4.2	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Chrome 34 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Firefox 29 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Googlebot Oct 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	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_RSA_WITH_AES_128_CBC_SHA (0x2f) No 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_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128

IE Mobile 11 / Win Phone 8.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 8b132	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
OpenSSL 1.0.1e	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	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	Not mitigated server-side (more info) SSL 3: 0x5, TLS 1.0: 0x2f
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	**No WEAK** (more info)
Next Protocol Negotiation	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Sun Jun 22 15:23:43 UTC 2014
Test duration	42.179 seconds
HTTP status code	302
HTTP forwarding	https://login.live.com
HTTP server signature	Microsoft-IIS/7.5
Server hostname	origin.sn145w.snt145.mail.live.com
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11

Copyright © 2009-2014 Qualys, Inc. All Rights Reserved. Terms and Conditions