QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > gmx.net > 213.165.65.50

SSL Report: gmx.net (213.165.65.50)

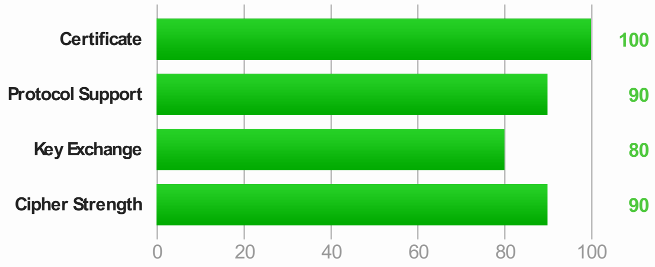
Assessed on: Sun Jun 22 09:21:13 UTC 2014 | Clear cache

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	gmx.net
Alternative names	gmx.cc gmx.co.in gmx.de gmx.info gmx.it gmx.lu gmx.org gmx.ph gmx.se gmx.sg gmx.tm gmx.tw gmx.li gmx.at gmx.biz gmx.com.tr gmx.ch gmx.dk gmx.net
Prefix handling	Non-prefixed access only, but DNS not configured for prefix
Valid from	Tue May 20 00:00:00 UTC 2014
Valid until	Thu May 19 23:59:59 UTC 2016 (expires in 1 year and 10 months)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	Thawte SSL 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 (3573 bytes)
Chain issues	None

#2

Subject	Thawte SSL CA SHA1: 73e42686657aece354fbf685712361658f2f4357
Valid until	Fri Feb 07 23:59:59 UTC 2020 (expires in 5 years and 7 months)

Key	RSA 2048 bits
Issuer	thawte Primary Root CA
Signature algorithm	SHA1withRSA

#3

Subject	thawte Primary Root CA SHA1: 1fa490d1d4957942cd23545f6e823d0000796ea2
Valid until	Wed Dec 30 23:59:59 UTC 2020 (expires in 6 years and 6 months)
Key	RSA 2048 bits
Issuer	Thawte Premium Server CA
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	gmx.net SHA1: 7a65a93a1a4732cba669f9d76d0e4197959f476a RSA 2048 bits / SHA1withRSA
2	Sent by server	Thawte SSL CA SHA1: 73e42686657aece354fbf685712361658f2f4357 RSA 2048 bits / SHA1withRSA
3	In trust store	thawte Primary Root CA SHA1: 91c6d6ee3e8ac86384e548c299295c756c817b81 RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	gmx.net SHA1: 7a65a93a1a4732cba669f9d76d0e4197959f476a RSA 2048 bits / SHA1withRSA
2	Sent by server	Thawte SSL CA SHA1: 73e42686657aece354fbf685712361658f2f4357 RSA 2048 bits / SHA1withRSA
3	Sent by server	thawte Primary Root CA SHA1: 1fa490d1d4957942cd23545f6e823d0000796ea2 RSA 2048 bits / SHA1withRSA
4	In trust store	Thawte Premium Server CA SHA1: 627f8d7827656399d27d7f9044c9feb3f33efa9a RSA 1024 bits / MD5withRSA 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_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	112
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_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	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_128_CBC_SHA (0x33) FS	128
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) 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_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Chrome 34 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Firefox 29 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Googlebot Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
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_3DES_EDE_CBC_SHA (0xa) No FS	112
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_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 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
OpenSSL 1.0.1e	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) 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	**Supported DoS DANGER** (more info)
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x33, TLS 1.0: 0x33
TLS compression	No
RC4	No
Heartbeat (extension)	No

Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	**TLS 1.3 TLS 1.98 TLS 2.98**
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Sun Jun 22 09:16:47 UTC 2014
Test duration	81.731 seconds
HTTP status code	301
HTTP forwarding	http://www.gmx.net
HTTP server signature	Apache
Server hostname	gmx.net
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11

Terms and Conditions