



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > posteo.de

SSL Report: posteo.de (89.146.220.134)

Assessed on: Mon Jun 23 02:32:38 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [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	www.posteo.de
Alternative names	www.posteo.de posteo.de m.posteo.de lists.posteo.de autodiscover.posteo.de mx01.posteo.de mx02.posteo.de mx03.posteo.de mx04.posteo.de
Prefix handling	Both (with and without WWW)
Valid from	Wed Apr 16 13:03:06 UTC 2014
Valid until	Sat Apr 16 16:23:04 UTC 2016 (expires in 1 year and 9 months)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	StartCom Extended Validation Server CA
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	2 (3547 bytes)
Chain issues	None
#2	
Subject	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274
Valid until	Tue Jan 01 06:00:00 UTC 2019 (expires in 4 years and 6 months)



Certification Paths

Path #1: Trusted

		www.posteo.de
1	Sent by server	SHA1: 3a89d8addca7235c8f44e9dd2e856a31d2d3c970 RSA2048 bits / SHA256withRSA
2	Sent by server	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274 RSA2048 bits / SHA1withRSA
3	In trust store	StartCom Certification Authority SHA1: a3f1333fe242bfcfc5d14e8f394298406810d1a0 RSA4096 bits / SHA256withRSA

Path #2: Trusted

		www.posteo.de
1	Sent by server	SHA1: 3a89d8addca7235c8f44e9dd2e856a31d2d3c970 RSA2048 bits / SHA256withRSA
2	Sent by server	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274 RSA2048 bits / SHA1withRSA
3	In trust store	StartCom Certification Authority SHA1: 3e2bf7f2031b96f38ce6c4d8a85d3e2d58476a0f RSA4096 bits / SHA1withRSA

Configuration



Protocols

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



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

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	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_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	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_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03f)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc03b)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc039)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0xc088)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02e)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0xc02d)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc02c)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0xc09a)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0xc045)	DH 1024 bits (p: 128, g: 1, Ys 128) FS	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH 256 bits (eq. 3072 bits RSA) FS	128

TLS_RSA_WITH_RC4_128_SHA(0x5) 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_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)	FS	256
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA(0x5)	No FS RC4	128
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)	FS	256
Chrome 34 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0xc02f)	FS	128
Firefox 24.2.0 ESR / Wn 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
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_AES_256_CBC_SHA(0xc014)	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_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
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 / Wn 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 11 / Wn 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(0xc027)	FS	128
IE 11 / Wn 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(0xc027)	FS	128
IE Mobile 10 / Wn Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE Mobile 11 / Wn 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_AES_128_CBC_SHA(0xc013)	FS	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_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)	FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)	FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
YandexBot May 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	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
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	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains
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 02:31:22 UTC 2014
Test duration	75.884 seconds
HTTP status code	301
HTTP forwarding	http://posteo.de
HTTP server signature	Apache
Server hostname	mail.posteo.de
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11