



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

SSL Report: navigator.web.de (217.72.194.207)

Assessed on: Mon Jun 23 08:05:27 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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	*.web.de
Alternative names	*.web.de
Prefix handling	Not required for subdomains
Valid from	Wed Apr 09 05:48:51 UTC 2014
Valid until	Tue Apr 14 23:59:59 UTC 2015 (expires in 9 months and 25 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	TeleSec ServerPass DE-2
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (4514 bytes)
Chain issues	Contains anchor
#2	
Subject	TeleSec ServerPass DE-2 SHA1: 98662c9a0d0947e3de928afe4c15c80b384e8cca
Valid until	Tue Jul 09 23:59:00 UTC 2019 (expires in 5 years)
Key	RSA2048 bits
Issuer	Deutsche Telekom Root CA2

Signature algorithm

SHA256withRSA

#3

Subject

Deutsche Telekom Root CA2 In trust store
SHA1: 85a408c09c193e5d51587dodd61330fd8cde37bf

Valid until

Tue Jul 09 23:59:00 UTC 2019 (expires in 5 years)

Key


RSA2048 bits

Issuer

Deutsche Telekom Root CA2 Self-signed

Signature algorithm

SHA1withRSA

 Certification Paths

Path #1: Trusted

1

Sent by server

*.web.de
SHA1: 302c44fcc58726fea8318824dec97c0a1a565888
RSA2048 bits / SHA256withRSA

2

Sent by server


TeleSec ServerPass DE-2
SHA1: 98662c9a0d0947e3de928afe4c15c80b384e8cca
RSA2048 bits / SHA256withRSA

3

Sent by server
In trust store

Deutsche Telekom Root CA2
SHA1: 85a408c09c193e5d51587dodd61330fd8cde37bf
RSA2048 bits / SHA1withRSA

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_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_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys 128) FS 256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys 128) FS 256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys 128) FS 256

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys 128) 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_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) 256

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS 112

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys 128) FS 112

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH 256 bits (eq. 3072 bits RSA) FS 128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) 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_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits (p: 128, g: 1, Ys 128) FS 128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits (p: 128, g: 1, Ys 128) FS 128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys 128) FS 128

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(0x45)	DH 1024 bits(p: 128, g: 1, Ys: 128)	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_CAMELLIA_128_CBC_SHA(0x41)			128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(0x16)	FS	112
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_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
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_256_CBC_SHA(0xc014)	FS	256
Firefox 24.2.0 ESR / Win 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_256_CBC_SHA(0xc014)	FS	256
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	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	No FS	112
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_3DES_EDE_CBC_SHA(0xa)	No FS	112
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Java 6u45 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(0x16)	FS	112
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(0xc012)	FS	112
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(0xc012)	FS	112
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.

(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: 0xc014, TLS 1.0: 0xc014
TLS compression	No
RC4	No
Heartbeat (extension)	Yes

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)	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 08:03:58 UTC 2014
Test duration	88.669 seconds
HTTP status code	403
HTTP server signature	Apache
Server hostname	navigator.web.de
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11