SSL Report: nsa.gov (23.63.180.226)

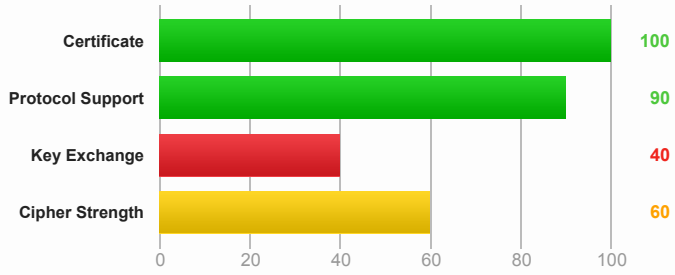
Assessed on: Thu May 08 21:52:57 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

C



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

This server is not vulnerable to the Heartbleed attack. (Experimental)

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

Authentication

Server Key and Certificate #1

Common names	www.nsa.gov
Alternative names	www2.nsa.gov www.nsa.gov nsa.gov
Prefix handling	Both (with and without WWW)
Valid from	Fri Apr 18 16:46:53 UTC 2014
Valid until	Tue Oct 21 04:48:03 UTC 2014 (expires in 5 months and 15 days)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	GeoTrust 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	2 (2317 bytes)
Chain issues	None

#2

Subject	GeoTrust SSL CA SHA1: 780a06f6e9b4061cad0c6502710606eb535f1c26
Valid until	Tue Feb 18 22:39:26 UTC 2020 (expires in 5 years and 9 months)

Valid until	Tue Feb 18 22:59:26 UTC 2020 (expires in 5 years and 9 months)
Key	RSA 2048 bits
Issuer	GeoTrust Global CA
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	www.nsa.gov SHA1: ac40f58487a796c69efc7d62f513f523a1cdd9c6 RSA 2048 bits / SHA1withRSA
2	Sent by server	GeoTrust SSL CA SHA1: 780a06f6e9b4061cad0c6502710606eb535f1c26 RSA 2048 bits / SHA1withRSA
3	In trust store	GeoTrust Global CA SHA1: de28f4a4ffe5b92fa3c503d1a349a7f9962a8212 RSA 2048 bits / SHA1withRSA

Configuration

Protocols

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

Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **WEAK**	40
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.3	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Android 4.4.2	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
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_256_CBC_SHA (0x35) No FS	256
Chrome 33 / Win 7 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256

Firefox 27 / Win 8 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Googlebot Oct 2013	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_RC4_128_MD5 (0x4) 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_MD5 (0x4) 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 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 8b132	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
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 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	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 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) No FS	256
YandexBot 3.0 No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112

(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: 0x6, TLS 1.0: 0x6
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbleed	No (more info)
Forward Secrecy	**No NOT DESIRABLE** (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	Thu May 08 21:52:21 UTC 2014
Test duration	36.499 seconds
HTTP status code	302
HTTP forwarding	http://www.nsa.gov

HTTP server signature	AkamaiGHost
Server hostname	a23-63-180-226.deploy.static.akamaitechnologies.com
PCI compliant	No
FIPS-ready	No

SSL Report v1.9.22