QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > indexinvestering.se

SSL Report: indexinvestering.se (194.14.207.134)

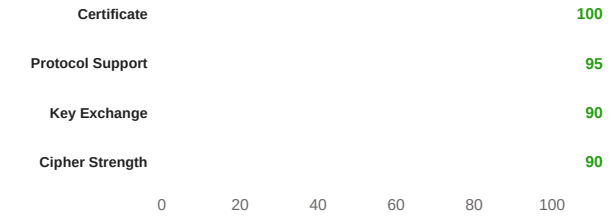
Assessed on: Wed, 07 Oct 2015 11:37:01 UTC | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

Authentication

Server Key and Certificate #1

Common names	www.indexinvestering.se
Alternative names	www.indexinvestering.se indexinvestering.se
Prefix handling	Both (with and without WWW)
Valid from	Thu, 10 Sep 2015 19:40:12 UTC
Valid until	Sun, 11 Sep 2016 21:09:14 UTC (expires in 11 months and 4 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL SHA256 CA - G4
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (2419 bytes)
Chain issues	None

#2

Subject	RapidSSL SHA256 CA - G4 Fingerprint: dc077c4ab3422f608cee83d9098bfc3a7226d6a7
Valid until	Sun, 29 Jun 2025 23:59:59 UTC (expires in 9 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	GeoTrust Primary Certification Authority - G3
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	www.indexinvestering.se Fingerprint: 04a5632fb04d45da9d2ddeaa5c3ddce32ff170b1 RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	RapidSSL SHA256 CA - G4 Fingerprint: dc077c4ab3422f608cee83d9098bfc3a7226d6a7 RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	GeoTrust Primary Certification Authority - G3 Self-signed Fingerprint: 039eedb80be7a03c6953893b20d2d9323a4c2afd RSA 2048 bits (e 65537) / SHA256withRSA

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; deprecated and SSL 2 suites at the end)

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 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits (p: 256, g: 1, Ys: 256) 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_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 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 2048 bits (p: 256, g: 1, Ys: 256) FS	112
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
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

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_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256

Handshake Simulation

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
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Baidu Jan 2015	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Chrome 43 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Firefox 39 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Googlebot Feb 2015	TLS 1.2	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_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_SHA384 (0xc028) FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Edge 12 / Win 10 (Build 10130) R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Java 6u45 No SNI [2]	Client does not support DH parameters > 1024 bits		Fail[3]
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 8u31	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 1.0.1l R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
OpenSSL 1.0.2 R	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 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 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Yahoo Slurp Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
YandexBot Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) 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
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes

Protocol Details

Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
Next Protocol Negotiation (NPN)	Yes http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Public Key Pinning (HPKP)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Wed, 07 Oct 2015 11:34:28 UTC
Test duration	153.973 seconds
HTTP status code	302
HTTP forwarding	**http://www.indexinvestering.se PLAINTEXT**
HTTP server signature	nginx
Server hostname	mailserver.indexinvestering.se

SSL Report v1.19.33