

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

SSL Report: securevcheck.com (216.224.175.101)

Assessed on: Sun, 28 Feb 2016 17:53:48 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A+

Certificate

Protocol Support

KeyExchange

Cipher Strength

0 20 40 60 80 100

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.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

Authentication



Server Key and Certificate #1

	www.securevcheck.com
Subject	Fingerprint SHA1: 18d40d7d7e648f1ba4631f1994d398c283b17a32 Pin SHA256: r3mz9nSwy6a+e8Mj1ZG5wel8cTf+IL4uVLi61qCHwl=
Common names	www.securevcheck.com
Alternative names	www.securevcheck.com securevcheck.com
Prefix handling	Both (with and without WWW)
Valid from	Tue, 11 Nov 2014 06:03:41 UTC
Valid until	Wed, 11 Jul 2018 10:07:34 UTC (expires in 2 years and 4 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL SHA256 CA - G3
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 (2286 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	RapidSSL SHA256 CA - G3
	Fingerprint SHA1: 0e34141846e7423d37f20dc0ab06c9bbd843dc24
	Pin SHA256: 6X0INAQIPijXKEVcqZBwyMcRwq1yW60549axatu3oDE=
Valid until	Fri, 20 May 2022 21:39:32 UTC (expires in 6 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	GeoTrust Global CA
Signature algorithm	SHA256withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	www.securevcheck.com
		Fingerprint SHA1: 18d40d7d7e648f1ba4631f1994d398c283b17a32
		Pin SHA256: r3mz9nSwy6a+e8Mj1ZG5wel8cTf+IL4uVLI61qCHwI= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	RapidSSL SHA256 CA - G3
		Fingerprint SHA1: 0e34141846e7423d37f20dc0ab06c9bbd843dc24
		Pin SHA256: 6X0INAQIPijXKEVcqZBwyMcRwq1yW60549axatu3oDE= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	GeoTrust Global CA Self-signed
		Fingerprint SHA1: de28f4a4fe5b92fa3c503d1a349a7f9962a8212
		Pin SHA256: h6801m+z8v3zbgkRHpq6L29Esgfzhj89C1SyUCOmqU= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

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 secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02e)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc03b)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc039)	DH 2048 bits FS	256



Handshake Simulation

Android 2.3.7	No SNI ²	Protocol or cipher suite mismatch
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Handshake Simulation

Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Baidu Jan 2015	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Chrome 47 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 42 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 6 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch			
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch			
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048	FS
IE 11 / Win 8.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048	FS
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048	FS
IE 11 / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 6u45 No SNI ²	Protocol or cipher suite mismatch			
Java 7u25	Protocol or cipher suite mismatch			
Java 8u31	Client aborts on SNI unrecognized_name warning			
	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 2048	FS
OpenSSL 1.0.1j R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
OpenSSL 1.0.2 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
YandexBot Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS

- (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 sometimes 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)

Protocol Details

Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Application-Layer Protocol Negotiation (ALPN)	No
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=63072000; includeSubDomains
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor securevcheck.com
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	securevcheck.com www.securevcheck.com
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Sun, 28 Feb 2016 17:52:21 UTC
Test duration	87.553 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.22 (Ubuntu)
Server hostname	vps-1151378-20014.manage.myhosting.com

SSL Report v 1.21.14