

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > secure.conscious.co.uk

SSL Report: secure.conscious.co.uk (83.222.239.226)

Assessed on: Wed Nov 05 13:05:01 PST 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

Category	Score
Certificate	100
Protocol Support	95
Key Exchange	90
Cipher Strength	90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is not vulnerable to the POODLE attack because it doesn't support SSL 3. [MORE INFO »](#)

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

Authentication

Server Key and Certificate #1

Common names	secure.conscious.co.uk
Alternative names	secure.conscious.co.uk
Prefix handling	Not required for subdomains
Valid from	Sun Oct 26 17:00:00 PDT 2014
Valid until	Fri Jun 22 16:59:59 PDT 2018 (expires in 3 years and 7 months)
Key	RSA 2048 bits
Weak key (Debian)	No
Issuer	Symantec Class 3 Secure Server CA - G4
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (2631 bytes)
Chain issues	None
#2	
Subject	Symantec Class 3 Secure Server CA - G4 SHA1: ff67367c5cd4de4ae18bce1d70fdabd7c866135
Valid until	Mon Oct 30 16:59:59 PDT 2023 (expires in 8 years and 11 months)
Key	RSA 2048 bits
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA256withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	secure.conscious.co.uk SHA1: abab6e501decf69b73f728d39b92c62ab2969712 RSA 2048 bits / SHA256withRSA
2	Sent by server	Symantec Class 3 Secure Server CA - G4 SHA1: ff67367c5cd4de4ae18bcce1d70fdabd7c866135 RSA 2048 bits / SHA256withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 RSA 2048 bits / SHA1withRSA Weak or insecure signature, but no impact on root certificates

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 always 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_SEED_CBC_SHA (0x9a)	DH 2048 bits (p: 256, g: 1, Ys: 256) FS	128
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_SEED_CBC_SHA (0x96)		128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

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
TLS_RSA_WITH_RC4_128_MD5 (0x4)			128

**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
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 Jun 2014		TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	FS	256
Chrome 37 / 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 32 / OS X	R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Googlebot Jun 2014		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_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_SHA384 (0xc028)	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		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 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 1.0.1h		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 8 / iOS 8.0 Beta	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 Jun 2014	No SNI ²	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	FS	256
YandexBot Sep 2014		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 attack	No, SSL 3 not supported (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
TLS compression	No

Protocol Details

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 (more info)
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	Wed Nov 05 13:03:02 PST 2014
Test duration	119.427 seconds
HTTP status code	403
HTTP server signature	Apache
Server hostname	cluster01.conscious.co.uk
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.36