

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > test.free-solutions.org

SSL Report: test.free-solutions.org (212.147.112.173)

Assessed on: Tue, 07 Mar 2017 17:47:28 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

B

Certificate

Protocol Support

Key Exchange

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 weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	test.free-solutions.org Fingerprint SHA1: cea16e53e413a19e471809ce72ed840f7b2fb752 Pin SHA256: lRCKGOO+qGG0UZojG+1bvwOeRbNmKRj9khguyPWz8aU=
Common names	test.free-solutions.org
Alternative names	test.free-solutions.org
Valid from	Tue, 10 Jan 2017 10:28:00 UTC
Valid until	Mon, 10 Apr 2017 10:28:00 UTC (expires in 1 month and 2 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
Revocation status	Good (not revoked)
DNS CAA	No
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	2 (2476 bytes)
Chain issues	None
#2	
Subject	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=

Additional Certificates (if supplied)

Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 4 years)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA



Certification Paths



[Click here to expand](#)

Certificate #2: DSA 1024 bits (SHA1withDSA)



Server Key and Certificate #1

Subject	test.free-solutions.org Fingerprint SHA1: 6b6109c14ff278b3b2e09221ddee2e0c98a6bc7c Pin SHA256: p/lboCvqQF4gB89aaHx4455Zn/lFtkAS0nxoz/YXaCU=
Common names	test.free-solutions.org
Alternative names	-
Valid from	Wed, 01 Jun 2016 11:09:42 UTC
Valid until	Mon, 31 May 2021 11:09:42 UTC (expires in 4 years and 2 months)
Key	DSA 1024 bits WEAK
Weak key (Debian)	No
Issuer	test.free-solutions.org Self-signed
Signature algorithm	SHA1withDSA WEAK
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No
Trusted	No NOT TRUSTED



Additional Certificates (if supplied)

Certificates provided	1 (758 bytes)
Chain issues	None



Certification Paths



[Click here to expand](#)

Configuration



Protocols

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



Cipher Suites

# TLS 1.2 (server has no preference)	
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112



Cipher Suites

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x13)	DH 1024 bits FS WEAK	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 1024 bits FS WEAK	112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH sect571r1 (eq. 15360 bits RSA) FS	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x32)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH sect571r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x40)	DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits FS WEAK	128
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0xa2)	DH 1024 bits FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH sect571r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH sect571r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x38)	DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH sect571r1 (eq. 15360 bits RSA) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x6a)	DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits FS WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits FS WEAK	256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0xa3)	DH 1024 bits FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH sect571r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH sect571r1 (eq. 15360 bits RSA) FS	256
# TLS 1.1 (server has no preference)		+
# TLS 1.0 (server has no preference)		+



Handshake Simulation

Android 2.3.7	No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.0.4		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH sect283k1 FS
Android 4.1.1		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH sect571r1 FS
Android 4.2.2		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH sect571r1 FS
Android 4.3		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH sect571r1 FS
Android 4.4.2		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1 FS
Android 5.0.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 6.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Baidu Jan 2015		RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
BingPreview Jan 2015		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1 FS
Chrome 49 / XP SP3		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 51 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Googlebot Feb 2015		RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH sect571r1 FS
IE 6 / XP	No FS ¹ No SNI ²	Server closed connection			
IE 7 / Vista		RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
IE 8 / XP	No FS ¹ No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
IE 8-10 / Win 7	R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win 7	R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS

Handshake Simulation

IE 11 / Win 8.1 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS	
IE 11 / Win Phone 8.1 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256	No FS	
IE 11 / Win Phone 8.1 Update <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Edge 13 / Win Phone 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Java 6u45 <small>No SNI</small> ²	Server closed connection				
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8v	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 1024	FS
OpenSSL 1.0.1l <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1	FS
OpenSSL 1.0.2e <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 <small>R</small>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 7 / OS X 10.9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / iOS 8.4 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / OS X 10.10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 9 / iOS 9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 9 / OS X 10.11 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / iOS 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Safari 10 / OS X 10.12 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH sect571r1	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

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	(1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	Yes
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x2f
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No

Protocol Details

OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
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	No
Uses common DH primes	Yes Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported EC Named Curves	sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp256k1, secp256r1, secp384r1, secp521r1 (Server has no preference)
SSL 2 handshake compatibility	No

**HTTP Requests**

1 <https://test.free-solutions.org/> (HTTP/1.1 200 OK)

**Miscellaneous**

Test date	Tue, 07 Mar 2017 17:45:44 UTC
Test duration	104.608 seconds
HTTP status code	200
HTTP server signature	Jetty(9.2.z-SNAPSHOT)
Server hostname	fix.112.147.212.vtx.ch

SSL Report v1.27.3