

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > 1099process.com

SSL Report: 1099process.com (192.169.137.25)

Assessed on: Fri, 17 Nov 2017 18:18:31 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A

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](#).

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.1099process.com Fingerprint SHA256: a55a53ccc7882afd310aa41df215dc188c2d7e8e51437a9e95038dc220060e41 Pin SHA256: ZZHL9pxpgha7vX/vyhSKzo665pOwDakGP6VfGhb0rjY=
Common names	www.1099process.com
Alternative names	www.1099process.com 1099process.com
Serial Number	51e3bbe5f3715ac8
Valid from	Mon, 08 May 2017 15:14:00 UTC
Valid until	Tue, 08 May 2018 15:14:00 UTC (expires in 5 months and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Go Daddy Secure Certificate Authority - G2 AIA: http://certificates.godaddy.com/repository/gdig2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.godaddy.com/gdig2s1-505.crl OCSP: http://ocsp.godaddy.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	2 (2580 bytes)
Chain issues	None
#2	
Subject	Go Daddy Secure Certificate Authority - G2 Fingerprint SHA256: 973a41276ffd01e027a2aad49e34c37846d3e976ff6a620b6712e33832041aa6 Pin SHA256: 8Rw90Ej3TtH8RRkrq+WYDS9n7IS03bk5bjP/UXPtAY8=

Additional Certificates (if supplied)

Valid until	Sat, 03 May 2031 07:00:00 UTC (expires in 13 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	Go Daddy Root Certificate Authority - G2
Signature algorithm	SHA256withRSA



Certification Paths

[Click here to expand](#)

Configuration



Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.



Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc9d)		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc9c)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0xc3d)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0xc3c)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0xc35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0xc2f)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK	112

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)



Handshake Simulation

Android 2.3.7 No SNI ?	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 secp521r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	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_256_CBC_SHA	ECDH secp384r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS

SSL Server Test: 1099process.com (Powered by Qualys SSL Labs)

Handshake Simulation

Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	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 secp521r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp384r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS	
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp521r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp521r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS	
OpenSSL 1.0.1i R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp521r1	FS

Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS¹ No SNI² Protocol mismatch (not simulated)

(1) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

(2) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(3) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(4) 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

DROWN

No, server keys and hostname not seen elsewhere with SSLv2

(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 website [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

No

Insecure Client-Initiated Renegotiation

No

BEAST attack

Not mitigated server-side ([more info](#)) TLS 1.0: 0xc014

SSL Server Test: 1099process.com (Powered by Qualys SSL Labs)

Protocol Details

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)
Ticketbleed (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	With modern browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	Yes
Supported Named Groups	secp521r1, secp384r1, secp256r1 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests



1 <https://1099process.com/> (HTTP/1.1 301 Moved Permanently)



Miscellaneous

Test date	Fri, 17 Nov 2017 18:17:43 UTC
Test duration	47.330 seconds
HTTP status code	301
HTTP forwarding	https://www.1099process.com
HTTP server signature	Microsoft-IIS/7.5
Server hostname	ip-192-169-137-25.ip.secureserver.net

SSL Report v1.29.7

Copyright © 2009-2017 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

Qualys is the leading provider of integrated [infrastructure security](#), [cloud infrastructure security](#), [endpoint security](#), [devsecops](#), [compliance](#) and [web app security](#) solutions.