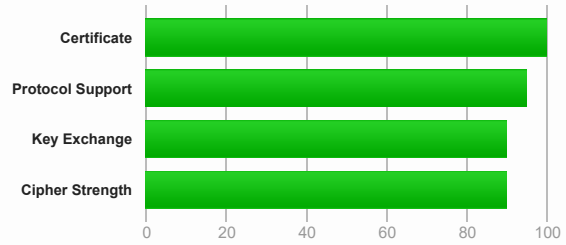
SSL Report: instagram.com (52.4.41.248)

Summary

Overall Rating

B



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

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	*.instagram.com Fingerprint SHA1: a5df95e765171830d685a014390cd0cdf3702a18 Pin SHA256: zoBWWPyGMJmYp0lbwbJW67VW9/u8Gc1OHYAu1dm1hrQ=
Common names	*.instagram.com
Alternative names	*.instagram.com *.cdninstagram.com *.igcdn.com *.igsonar.com cdninstagram.com igcdn.com igsonar.com instagram.com
Valid from	Wed, 08 Apr 2015 00:00:00 UTC
Valid until	Fri, 30 Dec 2016 12:00:00 UTC (expires in 7 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 High Assurance Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/sha2-ha-server-g5.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	2 (3050 bytes)
Chain issues	None

#2

Subject	DigiCert SHA2 High Assurance Server CA Fingerprint SHA1: a031c46782e6e6c662c2c87c76da9aa62ccabd8e Pin SHA256: k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=
Valid until	Sun, 22 Oct 2028 12:00:00 UTC (expires in 12 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert High Assurance EV Root CA

Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	*.instagram.com Fingerprint SHA1: a5df95e765171830d685a014390cd0cdf3702a18 Pin SHA256: zoBWWPyGMJmYp0lbwbJW67VW9/u8Gc1OHYAu1dm1hrQ= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	DigiCert SHA2 High Assurance Server CA Fingerprint SHA1: a031c46782e6e6c662c2c87c76da9aa62ccabd8e Pin SHA256: k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DigiCert High Assurance EV Root CA Self-signed Fingerprint SHA1: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25 Pin SHA256: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= 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_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH secp256r1 (eq. 3072 bits RSA) FS **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Baidu Jan 2015	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 48 / OS X R	RSA 2048 (SHA256)	TLS 1.2 > h2	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 42 / OS X R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
	RSA 2048 (SHA256)	TLS 1.2 > h2	

Firefox 44 / OS X R			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 secp256r1 FS
IE 6 / XP No FS [1] No SNI [2]	Server closed connection		
IE 7 / Vista	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 6u45 No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA1)	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_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA1)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 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

DROWN (experimental)	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 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	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
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	**Yes INSECURE** (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes

NPN	Yes h2 h2-fb http/1.1
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
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	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Sun, 29 May 2016 18:57:43 UTC
Test duration	85.507 seconds
HTTP status code	301
HTTP forwarding	https://www.instagram.com
HTTP server signature	proxygen
Server hostname	ec2-52-4-41-248.compute-1.amazonaws.com

SSL Report v1.22.37