Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > rubberduckiesftw.wpcomstaging.com

SSL Report: rubberduckiesftw.wpcomstaging.com (192.0.78.20)

Assessed on: Sun, 01 Dec 2024 03:32:27 UTC | **HIDDEN** | 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.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA384withECDSA)

Server Key and Certificate #1

Subject	wpcomstaging.com Fingerprint SHA256: 62f073741a40aae0740c72f86696958d3b46f84c3b8b1fee9f3d89f21a5a13b7 Pin SHA256: nBsH26DZfS0zlW0Baq4GpM0X4QUZUPXcY3mhG2Th85I=
Common names	wpcomstaging.com
Alternative names	*.wpcomstaging.com wpcomstaging.com
Serial Number	044339bee1dc7f03a059f2503666ef323e45
Valid from	Tue, 05 Nov 2024 01:25:40 UTC
Valid until	Mon, 03 Feb 2025 01:25:39 UTC (expires in 2 months and 1 day)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	E5 AIA: http://e5.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://e5.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: wpcomstaging.com issue: letsencrypt.org;validationmethods=dns-01;accounturi=https://acme-v02.api.letsencrypt.org/acme/acct/36334489 flags:0

Server Key and Certificate #1

Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2038 bytes)
Chain issues	None

#2

Subject	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years and 3 months)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	wpcomstaging.com Fingerprint SHA256: 62f073741a40aae0740c72f86696958d3b46f84c3b8b1fee9f3d89f21a5a13b7 Pin SHA256: nBsH26DZfS0zIW0Baq4GpM0X4QUZUPXcY3mhG2Th85I= EC 256 bits / SHA384withECDSA
2	Sent by server	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg= EC 384 bits / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Certificate #2: EC 256 bits (SHA384withECDSA) No SNI

Server Key and Certificate #1

Subject	wordpress.com Fingerprint SHA256: 86692b894bf29a07a239a646fc4eeae4c85dbb82559f1c09f61f76c8a1a963e2 Pin SHA256: WcLtppZeCQVuXMryuF+syrHHpTYg6GOU7NumWef1dLk=
Common names	wordpress.com
Alternative names	*.wordpress.com wordpress.com MISMATCH
Serial Number	0393a53d428a1ad18a1ddab186d892131f0b
Valid from	Wed, 13 Nov 2024 13:10:37 UTC
Valid until	Tue, 11 Feb 2025 13:10:36 UTC (expires in 2 months and 10 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	E5 AIA: http://e5.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://e5.o.lencr.org

Server Key and Certificate #1

Revocation status	Good (not revoked)
Trusted	No NOT TRUSTED Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2029 bytes)
Chain issues	None

#2

Subject	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years and 3 months)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (invalid certificate [Fingerprint SHA256: 86692b894bf29a07a239a646fc4eeae4c85dbb82559f1c09f61f76c8a1a963e2])

1	Sent by server	wordpress.com Fingerprint SHA256: 86692b894bf29a07a239a646fc4eeae4c85dbb82559f1c09f61f76c8a1a963e2 Pin SHA256: WcLtppZeCQVuXMryuF+syrHHpTYg6GOU7NumWef1dLk= EC 256 bits / SHA384withECDSA
2	Sent by server	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg= EC 384 bits / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Configuration

Protocols

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

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256

TLS 1.2 (suites in server-preferred order)

Cipher Suites

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256 (P)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Handshake Simulation

Android 4.4.2	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 5.0.0	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 8.0	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
BingPreview Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 49 / XP SP3	Server sent fatal alert: handshake_failure			
Chrome 69 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH x25519 FS
Googlebot Feb 2018	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
IE 11 / Win 7 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
IE 11 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 8u161	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.1l R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.2s R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 6 / iOS 6.0.1	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

Handshake Simulation

Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

 # Not simulated clients (Protocol mismatch)

Click here to expand

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

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc009
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc009
Sleeping POODLE	No (more info) TLS 1.2 : 0xc009
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV 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)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains; preload
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

Protocol Details

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	No
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://rubberduckiesftw.wpcomstaging.com/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sun, 01 Dec 2024 03:31:41 UTC
Test duration	46.349 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	-

SSL Report v2.3.0