Qualys. SSL Labs



# SSL Report: ecomm.codefusion.cf (35.227.125.200)

**Assessed on:** Sun, 13 Jan 2019 01:06:29 UTC **| HIDDEN** | Clear cache

## Summary

**Overall Rating**

**B**

**Certificate**

**Protocol Support**

**Key Exchange**

**Cipher Strength**

0

**Visit our documentation page for more information, configuration guides, and bool**

**This server's certificate chain is incomplete. Grade ca**

**Server sent invalid HSTS policy. See below for further i**

## Certificate #1: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

**Subject**

*.codefusion.cf

Fingerprint SHA256: fcec52cded43d6ff50ec77e0fab6d1

Pin SHA256: 0nNlSqm+LDfU2LFMyMR8wN7fGFpDr1S

## Server Key and Certificate #1

| | |
|---|---|
| **Common names** | *.codefusion.cf |
| **Alternative names** | *.codefusion.cf |
| **Serial Number** | 03a7cf1d072c2a3898a738a12ae61f8b1e38 |
| **Valid from** | Mon, 07 Jan 2019 00:07:09 UTC |
| **Valid until** | Sun, 07 Apr 2019 00:07:09 UTC (expires in 2 months and 24 da |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Let's Encrypt Authority X3<br>AIA: http://cert.int-x3.letsencrypt.org/ |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | **Yes (certificate)** |
| **OCSP Must Staple** | No |
| **Revocation information** | OCSP<br>OCSP: http://ocsp.int-x3.letsencrypt.org |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | **Yes**<br>**Mozilla Apple Android Java Windows** |

## Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 1 (1369 bytes) |
| **Chain issues** | **Incomplete** |

## Certification Paths

Mozilla | Apple | Android | Java | **Windows**

### Path #1: Trusted

| | | |
|---|---|---|
| **1** | Sent by server | *.codefusion.cf<br>Fingerprint SHA256: fcec52cded43d6ff50ec77e0fab6d101bc501<br>Pin SHA256: 0nNlSqm+LDfU2LFMyMR8wN7fGFpDr1SBQX9m |

Mozilla | Apple | Android | Java | Windows

| | | |
|---|---|---|
| | | RSA 2048 bits (e 65537) / SHA256withRSA |
| 2 | Extra download | Let's Encrypt Authority X3<br>Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c<br>Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=<br>RSA 2048 bits (e 65537) / SHA256withRSA |
| 3 | In trust store | DST Root CA X3 Self-signed<br>Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d92<br>Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=<br>RSA 2048 bits (e 65537) / SHA1withRSA<br>Weak or insecure signature, but no impact on root certificate |

# Configuration

## Protocols

TLS 1.3

TLS 1.2

TLS 1.1

TLS 1.0

SSL 3

SSL 2

For TLS 1.3 tests, we only support RFC 8446.

## Cipher Suites

**# TLS 1.2 (suites in server-preferred order)**

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bit

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA)

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS

## Cipher Suites

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**

TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**

**# TLS 1.1 (suites in server-preferred order)**

**# TLS 1.0 (suites in server-preferred order)**

## Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_ |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WI |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WI |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WI |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WI |
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WI |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WI |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WI |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WI |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WI |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WI |

## Handshake Simulation

| | | | |
|---|---|---|---|
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_CHACHA20 |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| IE 8 / XP No FS [1] No SNI [2] | Server sent fatal alert: handshake_failure | | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_GCM |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_128_GCM |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_C |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_128_GCM |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Java 6u45 No SNI [2] | Client does not support DH parameters > 1024 bits<br>RSA 2048 (SHA256) \| TLS 1.0 \| TLS_DHE_RSA_WITH_AES_128_CBC_SHA \| DH | | |
| Java 7u25 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| OpenSSL 1.0.2e R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_C |

## Handshake Simulation

| | | | |
|---|---|---|---|
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_C |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_G |

### # Not simulated clients (Protocol mismatch)

| | |
|---|---|
| IE 6 / XP No FS [1] No SNI [2] | Protocol mismatch (not simulated) |

(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

| | |
|---|---|
| **DROWN** | No, server keys and hostname not seen elsewhe<br>**(1) For a better understanding of this test, ple**<br>(2) Key usage data kindly provided by the Censys<br>(3) Censys data is only indicative of possible key |
| **Secure Renegotiation** | **Supported** |
| **Secure Client-Initiated Renegotiation** | No |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: 0x |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | No (more info) |
| **Downgrade attack prevention** | **Yes, TLS_FALLBACK_SCSV supported** (more |
| **SSL/TLS compression** | No |
| **RC4** | No |

## Protocol Details

| | |
|---|---|
| **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** | Yes h2 http/1.1 |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | **Invalid** **Server provided more than one HSTS header** |
| **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 |
| **DH public server param (Ys) reuse** | No |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | x25519, secp256r1, secp521r1, secp384r1 (server preferred orde |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1 **https://ecomm.codefusion.cf/** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Sun, 13 Jan 2019 01:04:32 UTC |
| **Test duration** | 116.928 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | nginx/1.14.0 + Phusion Passenger 6.0.1 |
| **Server hostname** | 200.125.227.35.bc.googleusercontent.com |

SSL Report v1.32.13

Copyright © 2009-2019 Qualys, Inc. All Rights Reserved.

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps,