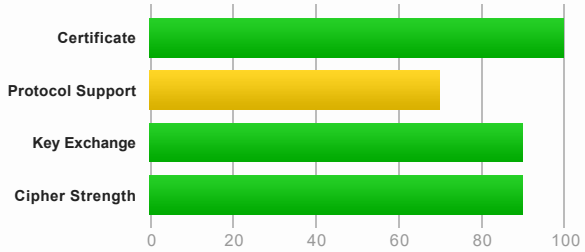
# SSL Report: www.yale.edu (104.16.243.46)

## Summary

Overall Rating


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

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

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

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

### Server Key and Certificate #1

| | |
|---|---|
| Subject | yale.edu<br>Fingerprint SHA256: fe73281d244e471b2281e23bba1c5fa97a29e6fcb806be3f703d2c2a01670388<br>Pin SHA256: 1w3ewDIqh3VJCTqkUilcASKkms77S0ZmkJT2OGqaj6U= |
| Common names | yale.edu |
| Alternative names | *.your.yale.edu housing.yalecollege.yale.edu *.housing.yalecollege.yale.edu *.housing-tst.yalecollege.yale.edu *.admissions.yale.edu yale.edu *.yale.edu *.news.yale.edu housing-tst.yalecollege.yale.edu |
| Serial Number | 075b88e3a36819a0ffad7868c37d30ac |
| Valid from | Mon, 04 Nov 2019 00:00:00 UTC |
| Valid until | Wed, 14 Oct 2020 12:00:00 UTC (expires in 7 months and 4 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | CloudFlare Inc RSA CA-1<br>AIA: http://cacerts.digicert.com/CloudFlareIncRSACA-1.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP<br>CRL: http://crl3.digicert.com/CloudFlareIncRSACA1.crl<br>OCSP: http://ocsp.digicert.com |
| Revocation status | Good (not revoked) |
| DNS CAA | No (more info) |
| Trusted | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 2 (2939 bytes) |
| Chain issues | None |

#2

| | |
|---|---|
| **Subject** | CloudFlare Inc RSA CA-1<br>Fingerprint SHA256: 328c5991d8383e27d0ebe910bf66c0af3d748a85d3011a52d88f1d8c8635647f<br>Pin SHA256: CfyancXuwYEHYRX3mmLJI3NFW6E8cydaCGS1D9wGhT4= |
| **Valid until** | Wed, 14 Oct 2020 12:00:00 UTC (expires in 7 months and 4 days) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | Baltimore CyberTrust Root |
| **Signature algorithm** | SHA256withRSA |

### Certification Paths

Click here to expand

## Certificate #2: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | ssl436760.cloudflaressl.com<br>Fingerprint SHA256: a9a3b4daf8b5759e6941b7942906c7eab36a807015330d6d67b3dc464ab39be2<br>Pin SHA256: fUk07XC0YL3HdWUWa9YEXdv8J05kaM1xscE7fAQH+Qk= |
| **Common names** | ssl436760.cloudflaressl.com |
| **Alternative names** | ssl436760.cloudflaressl.com *.yale.edu yale.edu |
| **Serial Number** | 009a44fe7e13bedbdee2ea87c66666ee54 |
| **Valid from** | Thu, 23 Jan 2020 00:00:00 UTC |
| **Valid until** | Fri, 31 Jul 2020 23:59:59 UTC (expires in 4 months and 22 days) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | COMODO RSA Domain Validation Secure Server CA 2<br>AIA: http://crt.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crt |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | Yes (certificate) |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL, OCSP<br>CRL: http://crl.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crl<br>OCSP: http://ocsp.comodoca4.com |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 3 (4551 bytes) |
| **Chain issues** | None |

#### #2

| | |
|---|---|
| **Subject** | COMODO RSA Domain Validation Secure Server CA 2<br>Fingerprint SHA256: ff201ca12c87a6f0cba643e9abb3c954c9155add3139b2e2eaed114bf9f75d31<br>Pin SHA256: EULHwYvGhknyznoBvyvgbidiBH3JX3eFHHIIO3YK8Ek= |
| **Valid until** | Mon, 24 Sep 2029 23:59:59 UTC (expires in 9 years and 6 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | COMODO RSA Certification Authority |
| **Signature algorithm** | SHA384withRSA |

#### #3

| | |
|---|---|
| **Subject** | COMODO RSA Certification Authority<br>Fingerprint SHA256: 4f32d5dc00f715250abcc486511e37f501a899deb3bf7ea8adbbd3aef1c412da<br>Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= |
| **Valid until** | Sat, 30 May 2020 10:48:38 UTC (expires in 2 months and 20 days) |
| **Key** | RSA 4096 bits (e 65537) |
| **Issuer** | AddTrust External CA Root |

| | |
|---|---|
| Signature algorithm | SHA384withRSA |

### Certification Paths

Click here to expand

## Certificate #3: EC 256 bits (SHA256withECDSA)

### Server Key and Certificate #1

| | |
|---|---|
| Subject | yale.edu<br>Fingerprint SHA256: bc8c22ba834632e9021e458d4179b52ae77c0564783dd634b82317f2d32f1f50<br>Pin SHA256: 7e/ZyqkaDoC0pZBCj3e0lekkVF4csOjRjVpzdaAnovk= |
| Common names | yale.edu |
| Alternative names | housing.yalecollege.yale.edu yale.edu *.admissions.yale.edu *.news.yale.edu *.housing.yalecollege.yale.edu *.yale.edu *.housing-tst.yalecollege.yale.edu *.your.yale.edu housing-tst.yalecollege.yale.edu |
| Serial Number | 0b6235610f0e23a358152b53f3c3f509 |
| Valid from | Mon, 04 Nov 2019 00:00:00 UTC |
| Valid until | Fri, 09 Oct 2020 12:00:00 UTC (expires in 6 months and 29 days) |
| Key | EC 256 bits |
| Weak key (Debian) | No |
| Issuer | CloudFlare Inc ECC CA-2<br>AIA: http://cacerts.digicert.com/CloudFlareIncECCCA-2.crt |
| Signature algorithm | SHA256withECDSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP<br>CRL: http://crl3.digicert.com/CloudFlareIncECCCA2.crl<br>OCSP: http://ocsp.digicert.com |
| Revocation status | Good (not revoked) |
| DNS CAA | No (more info) |
| Trusted | Yes<br>Mozilla Apple Android Java Windows |

### Additional Certificates (if supplied)

| | |
|---|---|
| Certificates provided | 2 (2344 bytes) |
| Chain issues | None |

#### #2

| | |
|---|---|
| Subject | CloudFlare Inc ECC CA-2<br>Fingerprint SHA256: 6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6<br>Pin SHA256: 3kcNJzkUJ1RqMXJzFX4Zxux5WfETK+uL6Viq9lJNn4o= |
| Valid until | Fri, 09 Oct 2020 12:00:00 UTC (expires in 6 months and 29 days) |
| Key | EC 256 bits |
| Issuer | Baltimore CyberTrust Root |
| 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 only support RFC 8446.

## Cipher Suites

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

| | |
|---|---|
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14) ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK | 128 |

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

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK | 256 |

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

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK | 256 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK | 112 |

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

## 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_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.4.2 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 5.0.0 | EC 256 (SHA256) | TLS 1.2 | OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Android 6.0 | EC 256 (SHA256) | TLS 1.2 > http/1.1 | OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS |
| Android 7.0 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |

| | | | |
|---|---|---|---|
| Android 8.0 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Android 8.1 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Android 9.0 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| BingPreview Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 69 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Chrome 70 / Win 10 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Chrome 75 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Firefox 31.3.0 ESR / Win 7 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Firefox 67 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Googlebot Feb 2018 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| IE 7 / Vista | RSA 2048 (SHA256) | 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 (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_128_CBC_SHA ECDH secp256r1 FS |
| IE 11 / Win 7 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | EC 256 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | EC 256 (SHA256) | 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 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 11 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Edge 15 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Edge 16 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Edge 18 / Win 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Edge 13 / Win Phone 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 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 secp256r1 FS |
| Java 8u161 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 11.0.3 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Java 12.0.1 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| OpenSSL 1.0.1l R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.0.2s R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| OpenSSL 1.1.0k R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS |
| OpenSSL 1.1.1c R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 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 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Safari 12.1.2 / MacOS 10.14.6 Beta R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Safari 12.1.1 / iOS 12.3.1 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Apple ATS 9 / iOS 9 R | EC 256 (SHA256) | TLS 1.2 > h2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| YandexBot Jan 2015 | EC 256 (SHA256) | TLS 1.2 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |

**# 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 elsewhere with SSLv2<br>**(1) For a better understanding of this test, please read this longer explanation**<br>(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here<br>(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) |
| **Zombie POODLE** | Unknown (more info) |
| **GOLDENDOODLE** | Unknown (more info) |
| **OpenSSL 0-Length** | Unknown (more info) |
| **Sleeping POODLE** | Unknown (more info) |
| **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** | With modern browsers (more info) |
| **ALPN** | Yes h2 http/1.1 |
| **NPN** | Yes h2 http/1.1 |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | Yes |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | **Yes**<br>max-age=31622400 |
| **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** | No |
| **Supported Named Groups** | x25519, secp256r1, secp384r1, secp521r1 (server preferred order) |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1 **https://www.yale.edu/** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 09 Mar 2020 19:15:34 UTC |
| **Test duration** | 92.809 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | cloudflare |
| **Server hostname** | - |

SSL Report v2.1.0

Copyright © 2009-2020 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.