

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

SSL Report: securevcheck.com (34.236.211.169)

Assessed on: Mon, 17 Feb 2020 16:57:39 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](#).

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 | www.securevcheck.com Fingerprint SHA256: 52e25341e8f5351a15c105f2a693433deb877a917ddb01db6f05d130f11b4307 Pin SHA256: T6m7ACHzWdJxPxGJ6YFoSsxkX+i9+C9YN+UaqKH0GFo= |
| Common names | www.securevcheck.com |
| Alternative names | www.securevcheck.com securevcheck.com |
| Serial Number | 6885972dc59c541224446a1c7b2f303c |
| Valid from | Fri, 20 Jul 2018 00:00:00 UTC |
| Valid until | Sun, 19 Jul 2020 23:59:59 UTC (expires in 5 months and 2 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | COMODO RSA Domain Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl OCSP: http://ocsp.comodoca.com |
| Revocation status | Good (not revoked) |
| DNS CAA | No (more info) |
| Trusted | Yes Mozilla Apple Android Java Windows |



Additional Certificates (if supplied)

| | |
|------------------------------|----------------|
| Certificates provided | 3 (4705 bytes) |
| Chain issues | None |

#2

Additional Certificates (if supplied)

| | |
|----------------------------|--|
| Subject | COMODO RSA Domain Validation Secure Server CA Fingerprint SHA256: 02ab57e4e67a0cb48dd2f34830e8ac40f4476fb08ca6be3f5cd846f646840f0 Pin SHA256: kIO23nT2ehFDXcfx3eHTDRESMz3asj1muO+4aldjiuY= |
| Valid until | Sun, 11 Feb 2029 23:59:59 UTC (expires in 8 years and 11 months) |
| Key | RSA 2048 bits (e 65537) |
| Issuer | COMODO RSA Certification Authority |
| Signature algorithm | SHA384withRSA |

#3

| | |
|----------------------------|--|
| Subject | COMODO RSA Certification Authority Fingerprint SHA256: 4f32d5dc00f715250abcc486511e37f501a899deb3bf7ea8adbbd3aef1c412da Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQG67CYDnvrLg5yRME= |
| Valid until | Sat, 30 May 2020 10:48:38 UTC (expires in 3 months and 12 days) |
| Key | RSA 4096 bits (e 65537) |
| Issuer | AddTrust External CA Root |
| Signature algorithm | SHA384withRSA |



Certification Paths

[Click here to expand](#)

Configuration



Protocols

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

For TLS 1.3 tests, we only support RFC 8446.



Cipher Suites

TLS 1.2 (server has no preference)



| | | |
|--|--|-----|
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | DH 2048 bits FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) | DH 2048 bits FS WEAK | 256 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | DH 2048 bits FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH secp521r1 (eq. 15360 bits RSA) FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) | DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) | DH 2048 bits FS | 256 |



Handshake Simulation

| | | | |
|-------------------------------|-------------------|--------------------|---|
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 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 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Android 8.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |
| Android 8.1 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS |

Handshake Simulation

| | | | | |
|--|-------------------|--------------------|---------------------------------------|-------------------|
| Android 9.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| Chrome 75 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 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 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| Firefox 67 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH x25519 FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_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_256_CBC_SHA384 | ECDH secp256r1 FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Java 11.0.3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Java 12.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 FS |
| OpenSSL 1.0.2s R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| OpenSSL 1.1.0k R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| OpenSSL 1.1.1c R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Safari 12.1.2 / MacOS 10.14.6 Beta R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Safari 12.1.1 / iOS 12.3.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH x25519 FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp384r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp521r1 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

DROWN

No, server keys and hostname not seen elsewhere with SSLv2

Protocol Details

| | |
|--|---|
| | <p>(1) For a better understanding of this test, please read this longer explanation</p> <p>(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here</p> <p>(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete</p> |
| 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: 0xc014 |
| GOLDENDOODLE | No (more info) TLS 1.2: 0xc014 |
| OpenSSL 0-Length | No (more info) TLS 1.2: 0xc014 |
| Sleeping POODLE | No (more info) TLS 1.2: 0xc014 |
| Downgrade attack prevention | Unknown (requires support for at least two protocols, excl. SSL2) |
| 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 http/1.1 |
| NPN | No |
| Session resumption (caching) | Yes |
| Session resumption (tickets) | Yes |
| OCSP stapling | No |
| Strict Transport Security (HSTS) | Yes max-age=31536000; includeSubDomains |
| 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 | secp256r1, secp384r1, secp521r1, x25519, x448 (Server has no preference) |
| SSL 2 handshake compatibility | Yes |



HTTP Requests



1 <https://securevcheck.com/> (HTTP/1.1 200 OK)



Miscellaneous

| | |
|-----------------------|-------------------------------|
| Test date | Mon, 17 Feb 2020 16:56:45 UTC |
| Test duration | 53.618 seconds |
| HTTP status code | 200 |
| HTTP server signature | Apache/2.4.29 (Ubuntu) |
| Server hostname | ls.securevcheck.com |

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.