

HomeProjectsQualys Free TrialContact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.defesa.pt

SSL Report: www.defesa.pt (194.140.232.58)

Assessed on: Sun, 24 Feb 2019 01:37:16 UTC | [Hide](#) | [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](#).


Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

| | |
|--------------------------|---|
| Subject | *.defesa.pt Fingerprint SHA256: 4e693e166df2deb8433bd0b45855877e1195e63882a08d6dfd9aebc2df246348 Pin SHA256: zfigRN+dtIH0J7SgZyABngBHPK2CwklK/ca9ACP6QnQ= |
| Common names | *.defesa.pt |
| Alternative names | *.defesa.pt defesa.pt |
| Serial Number | 1affb92d8afba75329d3548eab4b9fbe |
| Valid from | Thu, 09 Aug 2018 00:00:00 UTC |
| Valid until | Fri, 09 Aug 2019 23:59:59 UTC (expires in 5 months and 16 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | COMODO RSA Organization Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSARSAOrganizationValidationSecureServerCA.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL, OCSP CRL: http://crl.comodoca.com/COMODORSARSAOrganizationValidationSecureServerCA.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 (4796 bytes) |
| Chain issues | None |

#2

https://www.ssllabs.com/ssltest/analyze.html?d=www.defesa.pt

1/5

Additional Certificates (if supplied)

| | |
|---------------------|--|
| Subject | COMODO RSA Organization Validation Secure Server CA |
| | Fingerprint SHA256: 111006378afbe8e99bb02ba87390ca429fca2773f74d7f7eb5744f5ddf68014b |
| | Pin SHA256: EgNpQkIEUNXn9Ni6RoLOC532j1g5+EFw0ZpLxxJq9Ms= |
| Valid until | Sun, 11 Feb 2029 23:59:59 UTC (expires in 9 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: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvpRLg5yRME= |
| Valid until | Sat, 30 May 2020 10:48:38 UTC (expires in 1 year and 3 months) |
| 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 | 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_RSA_WITH_AES_256_CBC_SHA384 (0xc028) | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) | WEAK | | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) | WEAK | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | WEAK | | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | WEAK | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK | | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK | | 128 |
| # 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_RSA_WITH_AES_128_CBC_SHA | No FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 FS |

| Handshake Simulation | | | | | |
|--|--------------------------|---------|---------------------------------------|----------------|----|
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | 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 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| IE 8 / XP No FS ¹ No SNI ² | Server closed connection | | | | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp384r1 | FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp384r1 | FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | 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 secp521r1 | FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_256_CBC_SHA | No FS | |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| OpenSSL 1.0.2e R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp521r1 | FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp384r1 | FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp521r1 | 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

| | |
|--|--|
| | 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 website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete |
| DROWN | |
| BEAST attack | Not mitigated server-side (more info) TLS 1.0: 0xc014 |
| POODLE (SSLv3) | No, SSL 3 not supported (more info) |
| POODLE (TLS) | No (more info) |
| Downgrade attack prevention | No, TLS_FALLBACK_SCSV not 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) | Unknown (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 | No |
| NPN | No |
| Session resumption (caching) | No (IDs assigned but not accepted) |
| Session resumption (tickets) | No |
| OCSP stapling | No |
| Strict Transport Security (HSTS) | No |
| 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 | secp521r1, secp384r1, secp256r1 (server preferred order) |
| SSL 2 handshake compatibility | Yes |



HTTP Requests



- 1 https://www.defesa.pt/ (HTTP/1.1 302 Redirect)
- 2 https://www.defesa.pt/Paginas/Inicio.aspx (HTTP/1.1 200 OK)



Miscellaneous

| | |
|-----------------------|---|
| Test date | Sun, 24 Feb 2019 01:35:11 UTC |
| Test duration | 124.861 seconds |
| HTTP status code | 200 |
| HTTP server signature | Microsoft-IIS/7.5 Microsoft-HTTPAPI/2.0 |
| Server hostname | www.defesa.gov.pt |

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