

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

SSL Report: www.gymjil.cz (89.190.71.209)

Assessed on: Sat, 17 Feb 2024 15:00:07 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

C

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 server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server's certificate chain is incomplete. Grade capped to B.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

| | |
|---------------------------------|--|
| Subject | *.gymjil.cz Fingerprint SHA256: e5c90a772e7ee11d97b400ad231757162c0031a79b752024c198952d55ad1a1e Pin SHA256: SIQeRhDY+tko6Nbgorn1kPlgkta5pln9L5ej2U0F/s= |
| Common names | *.gymjil.cz |
| Alternative names | *.gymjil.cz gymjil.cz |
| Serial Number | 012789d04d416365f6b22c4eff5fc46 |
| Valid from | Wed, 15 Nov 2023 00:00:00 UTC |
| Valid until | Fri, 11 Oct 2024 23:59:59 UTC (expires in 7 months and 24 days) |
| Key | RSA 2048 bits (e 65537) |
| Weak key (Debian) | No |
| Issuer | Thawte RSA CA 2018 AIA: http://cacerts.thawte.com/ThawteRSACA2018.crt |
| Signature algorithm | SHA256withRSA |
| Extended Validation | No |
| Certificate Transparency | Yes (certificate) |
| OCSP Must Staple | No |
| Revocation information | CRL: OCSP CRL: http://odp.thawte.com/ThawteRSACA2018.crl OCSP: http://status.thawte.com |
| Revocation status | Good (not revoked) |
| DNS CAA | No (more info) |
| Trusted | Yes Mozilla Apple Android Java Windows |



Additional Certificates (if supplied)

| | |
|------------------------------|----------------|
| Certificates provided | 1 (1559 bytes) |
| Chain issues | Incomplete |



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 INSECURE | Yes |
| SSL 2 | No |



Cipher Suites

| | |
|--|-----|
| # TLS 1.2 (server has no preference) | |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK | 112 |
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 2048 bits FS WEAK | 112 |
| TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK | 112 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS WEAK | 128 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK | 128 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS WEAK | 128 |
| TLS_RSA_WITH_SEED_CBC_SHA (0x96) WEAK | 128 |
| TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 2048 bits FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS WEAK | 128 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK | 128 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE | 128 |
| TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH secp256r1 (eq. 3072 bits RSA) FS INSECURE | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS WEAK | 256 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK | 256 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK | 256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS WEAK | 256 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 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 secp256r1 (eq. 3072 bits RSA) FS WEAK | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| # TLS 1.1 (server has no preference) | |
| # TLS 1.0 (server has no preference) | |
| # SSL 3 (server has no preference) | |



Handshake Simulation

| | | | | | |
|---|-------------------|---------|------------------------------------|----------------|------------|
| Android 2.3.7 No SNI ² | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_RC4_128_SHA | No FS | RC4 |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |

Handshake Simulation

| | | | | | |
|--|-------------------|----------------|---------------------------------------|----------------|-----|
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 8.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 8.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Android 9.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 80 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | 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 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 73 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| IE 6 / XP No FS ¹ No SNI ² | RSA 2048 (SHA256) | SSL 3 | TLS_RSA_WITH_RC4_128_SHA | RC4 | |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA | No FS | |
| IE 8 / XP No FS ¹ No SNI ² | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_RC4_128_SHA | RC4 | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | 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 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA | No FS | |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_RSA_WITH_AES_128_CBC_SHA256 | No FS | |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 6u45 No SNI ² | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_RC4_128_SHA | No FS | RC4 |
| Java 7u25 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | 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 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | DH 2048 | FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | 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 secp256r1 | FS |
| OpenSSL 1.1.1c R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | 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 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | 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 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 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 | 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 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 12.1.1 / iOS 12.3.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | 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 secp256r1 | FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

Handshake Simulation

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(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

| | |
|---|--|
| | Unable to perform this test due to an internal error. (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 INTERNAL ERROR: test.drownattack.com INTERNAL ERROR: test.drownattack.com |
| DROWN | |
| Secure Renegotiation | Supported |
| Secure Client-Initiated Renegotiation | No |
| Insecure Client-Initiated Renegotiation | No |
| BEAST attack | Not mitigated server-side (more info) SSL 3: 0xa, TLS 1.0: 0xa |
| POODLE (SSLv3) | Vulnerable INSECURE (more info) SSL 3: 0xa |
| POODLE (TLS) | No (more info) |
| Zombie POODLE | No (more info) TLS 1.2: 0x000a |
| GOLDENDOODLE | No (more info) TLS 1.2: 0x000a |
| OpenSSL 0-Length | No (more info) TLS 1.2: 0x000a |
| Sleeping POODLE | No (more info) TLS 1.2: 0x000a |
| Downgrade attack prevention | Yes, TLS_FALLBACK_SCSV supported (more info) |
| SSL/TLS compression | No |
| RC4 | Yes INSECURE (more info) |
| Heartbeat (extension) | Yes |
| 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 some browsers (more info) |
| ALPN | No |
| NPN | No |
| Session resumption (caching) | Yes |
| Session resumption (tickets) | Yes |
| 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 |
| DH public server param (Ys) reuse | No |
| ECDH public server param reuse | No |
| Supported Named Groups | secp256r1 |
| SSL 2 handshake compatibility | Yes |



HTTP Requests



1 <https://www.gymjil.cz/> (HTTP/1.1 200 OK)



Miscellaneous

| | |
|------------------------------|-------------------------------|
| Test date | Sat, 17 Feb 2024 14:56:56 UTC |
| Test duration | 190.756 seconds |
| HTTP status code | 200 |
| HTTP server signature | Apache/2.4.7 (Ubuntu) |

Miscellaneous

Server hostname

-

SSL Report v2.2.0

Copyright © 2009-2024 [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.