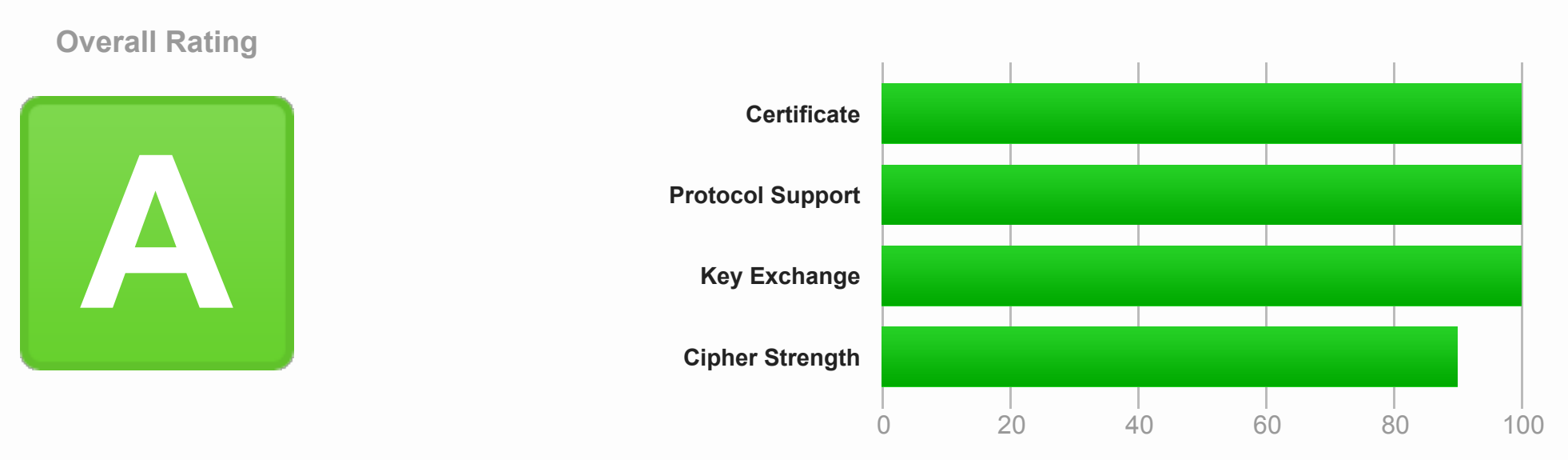
SSL Report: gondwana.majid.org (78.141.207.21)

Assessed on: Thu, 16 Sep 2021 10:32:03 UTC | HIDDEN | Clear cache

Scan Another »

Summary



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

This server supports TLS 1.3.

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	gondwana.majid.org Fingerprint SHA256: 3bf040f7bba69e0f812c4478cf6052e4b2ce9a77369b99a7236e795b54dffc9d Pin SHA256: zf3Z6T8+mkrk/ujozS5SVdAEw3ToSWcU64svPLmN5Wo=
Common names	gondwana.majid.org
Alternative names	gondwana.majid.org
Serial Number	03a3bea06e606f5934ed422bad682a05e40b
Valid from	Wed, 01 Sep 2021 16:38:38 UTC
Valid until	Tue, 30 Nov 2021 16:38:37 UTC (expires in 2 months and 14 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4267 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 3 years)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

Cipher Suites

TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH secp384r1 (eq. 7680 bits RSA) FS	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f) DH 4096 bits FS	256

Handshake Simulation

Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Android 5.0.0	Server sent fatal alert: handshake_failure		
Android 6.0	Server sent fatal alert: handshake_failure		
Android 7.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.0	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	Server sent fatal alert: handshake_failure		
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Googlebot Feb 2018	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 4096 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 16 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 18 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 8u161	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 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 (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
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)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (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	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)	Yes
OCSP stapling	Yes
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	secp384r1
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://gondwana.majid.org/ (HTTP/1.1 401 Unauthorized)

Miscellaneous

Test date	Thu, 16 Sep 2021 10:30:51 UTC
Test duration	71.666 seconds
HTTP status code	401
HTTP server signature	nginx/1.21.3
Server hostname	vpnukr.majid.org

SSL Report v2.1.8