SSL Report: www.mscbs.gob.es (195.64.186.177)

Assessed on: Fri, 22 Feb 2019 00:13:22 UTC | Hide | Clear cache

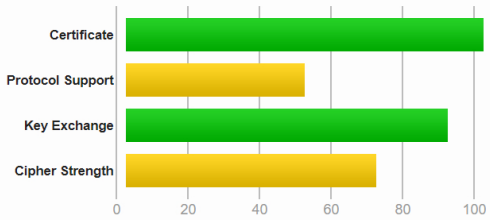
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

This server's certificate is not trusted by Apple and Java trust store (see below for details).

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	*.mscbs.gob.es Fingerprint SHA256: eca733f3f43c52863b7f7cf6ff9eddc92eb16b647b02e6b8af5dcee4576afbaa Pin SHA256: WEIE0OPKUMD6PDzCGa7AqXuCq6wplJml6LIQ+aE3zys=
Common names	*.mscbs.gob.es
Alternative names	*.mscbs.gob.es
Serial Number	4a1b64d876a4a5905b487fb92d615de1
Valid from	Fri, 13 Jul 2018 10:32:25 UTC
Valid until	Mon, 13 Jul 2020 10:32:24 UTC (expires in 1 year and 4 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	FNMT-RCM AIA: http://www.cert.fnmt.es/certs/ACCOMP.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://www.cert.fnmt.es/crlscomp/CRL1.crl OCSP: http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (5444 bytes)
Chain issues	Contains anchor

#2

Subject	FNMT-RCM / AC Componentes Informáticos Fingerprint SHA256: f038421f07f20d63a20d3691e5a178ab8459ebe570c1647b7690554ef23876ab Pin SHA256: MEJWDQI0WXBrEdYtj1u1WdwD26XslXQQ+57NkgXsoGc=

Valid until	Sat, 24 Jun 2028 10:52:59 UTC (expires in 9 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	FNMT-RCM / AC RAIZ FNMT-RCM
Signature algorithm	SHA256withRSA

#3

Subject	FNMT-RCM / AC RAIZ FNMT-RCM In trust store Fingerprint SHA256: ebc5570c29018c4d67b1aa127baf12f703b4611ebc17b7dab5573894179b93fa Pin SHA256: L8VmekuaJnjtasatJUZfy/YJS/zZUECXx6j6R63l6Ig=
Valid until	Tue, 01 Jan 2030 00:00:00 UTC (expires in 10 years and 10 months)
Key	RSA 4096 bits (e 65537)
Issuer	FNMT-RCM / AC RAIZ FNMT-RCM Self-signed
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	No
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 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp224r1 (eq. 2048 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp224r1 (eq. 2048 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp224r1 (eq. 2048 bits RSA) FS	**WEAK**	112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	**WEAK**	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	**WEAK**	112

 # 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_3DES_EDE_CBC_SHA No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 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	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 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 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 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 1.1	TLS_ECDHE_RSA_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	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp224r1 FS

 # Not simulated clients (Protocol mismatch)

IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
Apple ATS 9 / iOS 9 R	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 **(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
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)
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	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	Yes
Supported Named Groups	secp224r1, secp224k1, sect233k1, sect233r1, sect239k1, secp256r1, secp256k1, sect283k1, sect283r1, secp384r1, sect409k1, sect409r1, secp521r1, sect571k1, sect571r1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1 https://www.mscbs.gob.es/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Fri, 22 Feb 2019 00:11:08 UTC
Test duration	134.140 seconds
HTTP status code	200
HTTP server signature	server-header-none
Server hostname	-

SSL Report v1.32.16