

Qualys[®] SSL Labs

Home

Projects

Qualys.com

Contact

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

SSL Report: www.cm-braga.pt (62.28.4.75)

Assessed on: Mon, 19 Feb 2018 16:48:13 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 »](#)

Intermediate certificate has an insecure signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. [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 will be capped to B from March 2018. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	*.cm-braga.pt Fingerprint SHA256: 2d0eba2a84a6f57f7be1c930556ba40d34e7c0ba75dee65b9981b14d05fca38a Pin SHA256: qnFE4k+7FFRmqNCTIIYsObRImHvPos8qXfJyGQAfiw3E=
Common names	*.cm-braga.pt
Alternative names	*.cm-braga.pt cm-braga.pt
Serial Number	5eac03bad7317cb81dd27d909c0f3b25
Valid from	Fri, 28 Apr 2017 00:00:00 UTC
Valid until	Mon, 28 May 2018 23:59:59 UTC (expires in 3 months and 9 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL SHA256 CA AIA: http://gp.symcb.com/gp.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://gp.symcb.com/gp.crl OCSP: http://gp.symcd.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 (3394 bytes)
-----------------------	----------------

https://www.ssllabs.com/ssltest/analyze.html?d=www.cm-braga.pt

1/6

Additional Certificates (if supplied)

Chain issues	None
#2	
Subject	RapidSSL SHA256 CA Fingerprint SHA256: e6683e88315cd1cb403c0cea490f7c4b4c82c91cd485037489aadbaa90839f61 Pin SHA256: Slt48lBVTjuRQJTjbzopminRrHSGtndY0/sj0lF9Qk=
Valid until	Fri, 20 May 2022 23:45:51 UTC (expires in 4 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	GeoTrust Global CA
Signature algorithm	SHA256withRSA
#3	
Subject	GeoTrust Global CA Fingerprint SHA256: 3c35cc963eb004451323d3275d05b353235053490d9cd83729a2faf5e7ca1cc0 Pin SHA256: h6801m+z8v3zbgkRHpq6L29Esgfzhj89C1SyUCOQmqU=
Valid until	Tue, 21 Aug 2018 04:00:00 UTC (expires in 6 months and 1 day)
Key	RSA 2048 bits (e 65537)
Issuer	Equifax / Equifax Secure Certificate Authority
Signature algorithm	SHA1withRSA INSECURE



Certification Paths



[Click here to expand](#)

Certificate #2: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	*.cm-braga.pt Fingerprint SHA256: cc96444baab4def45961ab3fadebe852a8ca53fc5a6be9f7e661096c5850d03e Pin SHA256: /4+1QqjTCGDAKTF3rKdzj135Z7p5Bec/BcRqUP9Jvxw=
Common names	*.cm-braga.pt
Alternative names	*.cm-braga.pt cm-braga.pt
Serial Number	6127c3a3a79b6be0506f05f2c8a8ca2d
Valid from	Fri, 17 Jul 2015 00:00:00 UTC
Valid until	Sat, 16 Jul 2016 23:59:59 UTC (expired 1 year and 7 months ago) EXPIRED
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	No
OCSF Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl OCSP: http://ocsp.comodoca.com
Revocation status	Unchecked (only trusted certificates can be checked)
DNS CAA	No (more info)
Trusted	No NOT TRUSTED Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	1 (1362 bytes)
Chain issues	Incomplete




Certification Paths



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
For TLS 1.3 tests, we currently support draft version 18.		



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 secp521r1 (eq. 15360 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	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	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 secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	INSECURE	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	INSECURE	128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	WEAK	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH secp521r1 (eq. 15360 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	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	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 secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp521r1 (eq. 15360 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		
----------------------	--	--

Handshake Simulation

Android 2.3.7 No SNI²	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 secp256k1	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
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_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	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
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 secp521r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 57 / Win 7 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 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp521r1	FS
IE 6 / XP No FS¹ No SNI²	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 FS¹ No SNI²	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 13 / 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 SNI²	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 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	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 secp521r1	FS
OpenSSL 1.0.2e 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
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 secp384r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp521r1	FS

(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.

(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

	IP Address	Port	Export	Special	Status
	62.28.4.76	443	Yes	No	Not vulnerable
DROWN	<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 incomplete</p> <p>(4) We perform real-time key reuse checks, but stop checking after first confirmed vulnerability</p> <p>(5) The "Special" column indicates vulnerable OpenSSL version; "Export" refers to export cipher suites</p>				
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)				
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	secp256k1, secp256r1, secp384r1, secp521r1 (Server has no preference)				
SSL 2 handshake compatibility	Yes				



HTTP Requests



- 1 <https://www.cm-braga.pt/> (HTTP/1.1 302 Found)
- 2 <https://www.cm-braga.pt/en> (HTTP/1.1 200 OK)



Miscellaneous

Test date	Mon, 19 Feb 2018 16:45:19 UTC
Test duration	174.759 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	mail.cm-braga.pt

SSL Report v1.30.8

Copyright © 2009-2018 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

Qualys is the leading provider of integrated [infrastructure security](#), [cloud infrastructure security](#), [endpoint security](#), [devsecops](#), [compliance](#) and [web app security](#) solutions.