SSL Report: hbchrcm.tmc.gov.in (117.236.99.36)

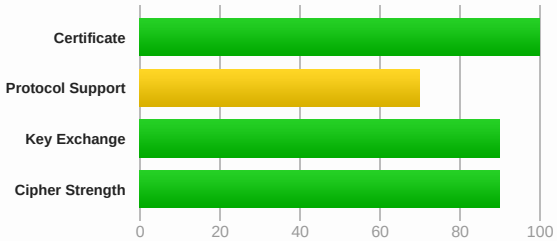
Assessed on: Sun, 25 Oct 2026 09:08:21 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This server does not support TLS 1.3. MORE INFO »

This server does not support PQC (Post-Quantum Cryptography) key exchange.

Certificate #1: RSA 4096 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	*.hbchrcm.tmc.gov.in Fingerprint SHA256: 767fef4f8f58a72300418cf1a36df8f3ecb1901781b132e8c1b5760fcd7b0fe2 Pin SHA256: Lef4Z+xKlFd6i8M2kVmzQRodvhjBEOgogBxamhUmAFo=
Common names	*.hbchrcm.tmc.gov.in
Alternative names	hbchrcm.tmc.gov.in *.hbchrcm.tmc.gov.in
Serial Number	3f1be3107fe5e3ca20a54e7fb55899
Valid from	Fri, 16 Oct 2026 09:09:53 UTC
Valid until	Wed, 13 Jan 2027 09:09:53 UTC (expires in 2 months and 19 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	EM DV TLS CA - G2A-1 AIA: http://repository.emsign.com/certs/EMDVTLSCAG2A1EE.p7c
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?EMDVTLSCAG2A1.crl OCSP: http://ocsp-a.emsign.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 (5329 bytes)
Chain issues	None

#2

Subject	EM DV TLS CA - G2A-1 Fingerprint SHA256: 3f13597d3355d341bd09328aee567d7f4e002d9919b986f9962daff197ea75d1 Pin SHA256: zrUpja649ZJ5SAtGACyJ93Vcw6FpUUsRuBC+/BlaANg=
Valid until	Mon, 28 May 2040 07:16:12 UTC (expires in 13 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root TLS CA - G1
Signature algorithm	SHA384withRSA

#3

Subject	emSign Root TLS CA - G1 Fingerprint SHA256: 9b913476eab476e21e0887dbcde44345d1359d28116b83b7cd3e87bd807ebf68 Pin SHA256: 7OKONSic6GIcckB5SeUFAFKtRgfMMy6vm1RgKarL+3o=
Valid until	Sat, 09 Jul 2039 18:30:00 UTC (expires in 12 years and 8 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root CA - G1
Signature algorithm	SHA256withRSA

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

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp384r1 (eq. 7680 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	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

Cipher Suites

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	**WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	**WEAK**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	**WEAK**	112

 # 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 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS	
Android 4.0.4	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Android 4.1.1	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Android 4.2.2	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Android 4.3	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Android 4.4.2	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Android 5.0.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Android 8.0	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Android 8.1	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Android 9.0	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Baidu Jan 2015	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
BingPreview Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Chrome 70 / Win 10	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Chrome 80 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Chrome 131 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 73 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Firefox 135 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Googlebot Feb 2018	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
IE 7 / Vista	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 8 / XP No FS [1] No SNI [2]	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
IE 8-10 / Win 7 R	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 2048 FS
IE 11 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 16 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 18 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 131 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 6u45 No SNI [2]	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS	
Java 7u25	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS

Handshake Simulation

Java 8u161	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 11.0.3	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Java 12.0.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 0.9.8y	RSA 4096 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
OpenSSL 1.0.1l R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
OpenSSL 1.1.1c R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Opera 117 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp384r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA384)	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	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 FS
YandexBot Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp384r1 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

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
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)
Zombie POODLE	No (more info) TLS 1.2 : `0xc027`
GOLDENDOODLE	No (more info) TLS 1.2 : `0xc027`
OpenSSL 0-Length	No (more info) TLS 1.2 : `0xc027`
Sleeping POODLE	No (more info) TLS 1.2 : `0xc027`
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)

Protocol Details

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	Yes h2 http/1.1
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
DH public server param (Ys) reuse	No
ECDH public server param reuse	**Yes**
Supported Named Groups	secp384r1, x25519, secp256r1 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://hbchrcm.tmc.gov.in/** (HTTP/1.1 403 Forbidden)

Miscellaneous

Test date	Sun, 25 Oct 2026 09:04:53 UTC
Test duration	208.700 seconds
HTTP status code	403
HTTP server signature	-
Server hostname	-

SSL Report v2.4.3

Copyright © 2009-2026 Qualys, Inc. All Rights Reserved. Privacy Policy. 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.