

CHECKING HOST(S) AVAILABILITY

mra-ims.celloscope.net:443

=> 103.23.41.212

SCAN RESULTS FOR MRA-IMS.CELLOSCOPE.NET:443 - 103.23.41.212

* Deflate Compression:

OK - Compression disabled

* TLS 1.0 Cipher Suites:

Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* SSL 3.0 Cipher Suites:

Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* Session Renegotiation:

Client Renegotiation DoS Attack: OK - Not vulnerable

Secure Renegotiation: OK - Supported

* Certificates Information:

Hostname sent for SNI: mra-ims.celloscope.net

Number of certificates detected: 1

Certificate #0 (_RSAPublicKey)

SHA1 Fingerprint: 31fdc93bb28ca09c724d5c660cf620d3be0cea21

Common Name: mra-ims.celloscope.net

Issuer: R3

Serial Number: 327266787009156183777642726498459021897735

Not Before: 2023-07-01

Not After: 2023-09-29

Public Key Algorithm: _RSAPublicKey

Signature Algorithm: sha256

Key Size: 2048

Exponent: 65537

DNS Subject Alternative Names: ['mra-ims.celloscope.net']

Certificate #0 - Trust

Hostname Validation: OK - Certificate matches server hostname

Android CA Store (9.0.0_r9): OK - Certificate is trusted

Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14): OK - Certificate is

trusted

Java CA Store (jdk-13.0.2): OK - Certificate is trusted

Mozilla CA Store (2021-01-24): OK - Certificate is trusted

Windows CA Store (2021-02-08): OK - Certificate is trusted

Symantec 2018 Deprecation: OK - Not a Symantec-issued certificate

Received Chain: mra-ims.celloscope.net --> R3 --> ISRG Root X1

Verified Chain: mra-ims.celloscope.net --> R3 --> ISRG Root X1

Received Chain Contains Anchor: OK - Anchor certificate not sent

Received Chain Order: OK - Order is valid

Verified Chain contains SHA1: OK - No SHA1-signed certificate in the verified certificate

chain

Certificate #0 - Extensions

OCSP Must-Staple: NOT SUPPORTED - Extension not found

Certificate Transparency: WARNING - Only 2 SCTs included but Google recommends 3 or

more

Certificate #0 - OCSP Stapling

NOT SUPPORTED - Server did not send back an OCSP response

* Downgrade Attacks:

TLS_FALLBACK_SCSV: OK - Supported

* TLS 1.1 Cipher Suites:
Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* OpenSSL CCS Injection:
OK - Not vulnerable to OpenSSL CCS injection

* TLS 1.2 Cipher Suites:
Attempted to connect using 156 cipher suites.

The server accepted the following 6 cipher suites:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256	ECDH: prime256v1 (256 bits)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256	ECDH: prime256v1 (256 bits)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256	ECDH: prime256v1 (256 bits)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128	ECDH: prime256v1 (256 bits)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128	ECDH: prime256v1 (256 bits)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128	ECDH: prime256v1 (256 bits)

The group of cipher suites supported by the server has the following properties:

Forward Secrecy	OK - Supported
Legacy RC4 Algorithm	OK - Not Supported

* TLS 1.3 Cipher Suites:
Attempted to connect using 5 cipher suites.

The server accepted the following 3 cipher suites:

TLS_CHACHA20_POLY1305_SHA256	256	ECDH: X25519 (253 bits)
TLS_AES_256_GCM_SHA384	256	ECDH: X25519 (253 bits)
TLS_AES_128_GCM_SHA256	128	ECDH: X25519 (253 bits)

* OpenSSL Heartbleed:
OK - Not vulnerable to Heartbleed

* ROBOT Attack:
OK - Not vulnerable, RSA cipher suites not supported.

* SSL 2.0 Cipher Suites:
Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

* TLS 1.2 Session Resumption Support:
With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
With TLS Tickets: OK - Supported.

* Elliptic Curve Key Exchange:
Supported curves: X25519, X448, prime256v1, secp384r1, secp521r1
Rejected curves: prime192v1, secp160k1, secp160r1, secp160r2, secp192k1,
secp224k1, secp224r1, secp256k1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1,
sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1

SCAN COMPLETED IN 58.59 S
