SSL Report: www.ua.pt (193.136.173.81)

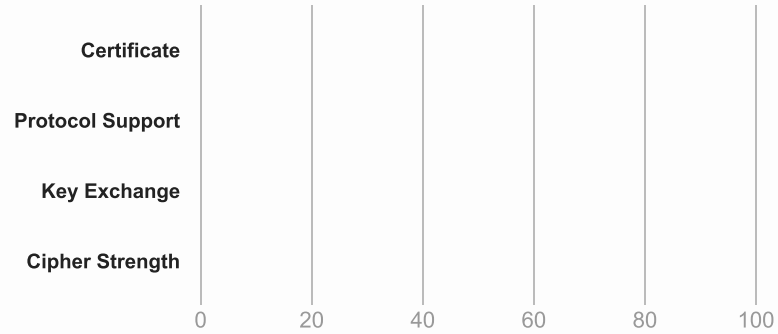
Assessed on: Mon, 18 Feb 2019 16:09:01 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



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

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

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »

Certificate #1: RSA 3072 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	*.ua.pt Fingerprint SHA256: c294912a2f3e9cb86a414e421596fe8deab4c014f6faa4464c6a48af1c7aa428 Pin SHA256: FegK/EZaHQg80+TinvkTlln09V1G24wYkFQha0XxIPE=
Common names	*.ua.pt
Alternative names	*.ua.pt ua.pt
Serial Number	04e32bc894dde0785ffcf4cb99f31bda
Valid from	Fri, 22 Jun 2018 00:00:00 UTC
Valid until	Fri, 26 Jun 2020 12:00:00 UTC (expires in 1 year and 4 months)
Key	RSA 3072 bits (e 65537)
Weak key (Debian)	No
Issuer	TERENA SSL CA 3 AIA: http://cacerts.digicert.com/TERENASSLCA3.crt
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/TERENASSLCA3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (3100 bytes)
Chain issues	None

#2

Additional Certificates (if supplied)

Subject	TERENA SSL CA 3 Fingerprint SHA256: beb8efe9b1a73c841b375a90e5fff8048848e3a2af66f6c4dd7b938d6fe8c5d8 Pin SHA256: 8651wEkMkH5ftiaLp57oqmx3KHTFzDgp7ZeJXR0ToBs=
Valid until	Mon, 18 Nov 2024 12:00:00 UTC (expires in 5 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Assured ID Root CA
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

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
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 3072 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS	
Android 4.0.4	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.1.1	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.2.2	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.3	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 4.4.2	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 5.0.0	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS
Android 6.0	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Android 7.0	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp384r1 FS
Baidu Jan 2015	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp521r1 FS

Handshake Simulation

BingPreview Jan 2015	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Chrome 49 / XP SP3	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
Chrome 69 / Win 7 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
Chrome 70 / Win 10	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 47 / Win 7 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 49 / XP SP3	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 62 / Win 7 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Googlebot Feb 2018	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
IE 7 / Vista	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
IE 8 / XP No FS [1] No SNI [2]	RSA 3072 (SHA384)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
IE 11 / Win 7 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
IE 11 / Win 8.1 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
IE 10 / Win Phone 8.0	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
IE 11 / Win Phone 8.1 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp384r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
IE 11 / Win 10 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
Edge 15 / Win 10 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
Java 6u45 No SNI [2]	RSA 3072 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp521r1 FS
Java 8u161	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
OpenSSL 0.9.8y	RSA 3072 (SHA384)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
OpenSSL 1.0.2e R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS

Handshake Simulation

Safari 5.1.9 / OS X 10.6.8	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Safari 6 / iOS 6.0.1	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 3072 (SHA384)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Safari 7 / iOS 7.1 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 7 / OS X 10.9 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 8 / iOS 8.4 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 8 / OS X 10.10 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 9 / iOS 9 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 9 / OS X 10.11 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 10 / iOS 10 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Safari 10 / OS X 10.12 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Apple ATS 9 / iOS 9 R	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 FS
Yahoo Slurp Jan 2015	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	RSA 3072 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp521r1 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

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: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
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)
OpenSSL CCS vuln. (CVE-2014-0224)	Unknown (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)	Yes
Session resumption (tickets)	No
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)

Protocol Details

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	secp521r1, secp384r1, secp256r1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://www.ua.pt/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Mon, 18 Feb 2019 16:06:15 UTC
Test duration	165.650 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/7.5
Server hostname	web-i.ua.pt

SSL Report v1.32.16