Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.

Summary of uptc.metalibros.org:443 (HTTPS) SSL Security Test

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website.
SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer: Let's Encrypt Authority X3
Trusted: Yes
Common Name: uptc.metalibros.org
Key Type/Size: RSA 2048 bits
Signature Algorithm: sha256WithRSAEncryption
Subject Alternative Names: DNS:libros-uptc.metabiblioteca.com.co, DNS:uptc.metalibros.org
Transparency: Yes
Validation Level: DV
CRL: No
OCSP: http://ocsp.int-x3.letsencrypt.org
OCSP Must-Staple: No
Supports OCSP Stapling: Yes
Valid From: May 6th 2020, 16:42 CEST
Valid To: August 4th 2020, 16:42 CEST

CERTIFICATE CHAIN

DST Root CA X3
Key Type/Size: RSA 2048 bits
Signature Algorithm: sha1WithRSAEncryption
SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ff6d9206d11bcd6770739
PIN: Vjs8r4z+80wjNcr1YKepWQboSIRi63WxhIMN+eWys=
Expires in: 485 days

Let's Encrypt Authority X3
Key Type/Size: RSA 2048 bits
Signature Algorithm: sha256WithRSAEncryption
SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
PIN: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBF2Fulhg=
Expires in: 288 days

uptc.metalibros.org
Key Type/Size: RSA 2048 bits
Signature Algorithm: sha256WithRSAEncryption
SHA256
94c4c27291d3137dedcb0591ee389cbfad5e508e2d9dbcc8bb71d65babee835a8
PIN
DnCabazPvq3vurv7LtvHtnUz8IeYXw0+HlpRk4uo630=
Expires in
63 days
Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

**CERTIFICATES ARE TRUSTED**

All the certificates provided by the server are trusted. 

**SUPPORTED CIPHERS**

List of all cipher suites supported by the server:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good</td>
</tr>
</tbody>
</table>

**SUPPORTED PROTOCOLS**

List of all SSL/TLS protocols supported by the server:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>Good</td>
</tr>
</tbody>
</table>

**DIFFIE-HELLMAN PARAMETER SIZE**

Diffie-Hellman parameter size: 2048 bits

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

<table>
<thead>
<tr>
<th>Elliptic Curve</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256</td>
<td>Good</td>
</tr>
</tbody>
</table>

**POODLE OVER TLS**

The server is not vulnerable to POODLE over TLS.

**GOLDENDOODLE**

The server is not vulnerable to GOLDENDOODLE.

**ZOMBIE POODLE**

The server is not vulnerable to Zombie POODLE.

**SLEEPING POODLE**

The server is not vulnerable to Sleeping POODLE.

**0-LENGTH OPENSSL**

The server is not vulnerable 0-Length OpenSSL.

**CVE-2016-2107**
The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).

**SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION**

The server does not support client-initiated insecure renegotiation.

**ROBOT**

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability.

**HEARTBLEED**

The server version of OpenSSL is not vulnerable to Heartbleed attack.

**CVE-2014-0224**

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).
Test For Compliance With HIPAA Guidance

Reference: HIPAA of 1996, Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

**X.509 CERTIFICATES ARE IN VERSION 3**
All the X509 certificates provided by the server are in version 3. **Good configuration**

**SERVER SUPPORTS OCSP STAPLING**
The server supports OCSP stapling, which allows better verification of the certificate validation status. **Good configuration**

**SUPPORTED PROTOCOLS**
List of all SSL/TLS protocols supported by the server:

- **TLSv1.2** **Good configuration**

**SUPPORTED CIPHERS**
List of all cipher suites supported by the server:

- **TLSv1.2** **Good configuration**
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **Good configuration**
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **Good configuration**
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 **Good configuration**
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **Good configuration**

**DIFFIE-HELLMAN PARAMETER SIZE**
Diffie-Hellman parameter size: **2048 bits** **Good configuration**

**SUPPORTED ELLIPTIC CURVES**
List of all elliptic curves supported by the server:

- **P-256 (prime256v1) (256 bits)** **Good configuration**

**EC_POINT_FORMAT EXTENSION**
The server supports the EC_POINT_FORMAT TLS extension. **Good configuration**
Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 2 - Section 3

**X.509 CERTIFICATES ARE IN VERSION 3**

All the X509 certificates provided by the server are in version 3. Good configuration

**SERVER SUPPORTS OCSP STAPLING**

The server supports OCSP stapling, which allows better verification of the certificate validation status. Good configuration

**SUPPORTED CIPHERS**

List of all cipher suites supported by the server:

**TLSv1.2**

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 Good configuration
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Good configuration

**SUPPORTED PROTOCOLS**

List of all SSL/TLS protocols supported by the server:

- TLSv1.2 Good configuration

**DIFFIE-HELLMAN PARAMETER SIZE**

Diffie-Hellman parameter size: 2048 bits Good configuration

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

- P-256 (prime256v1) (256 bits) Good configuration

**SERVER DOES NOT SUPPORT OF TLSV1.3**

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses. Information

**SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET**

The server does not support Extended Master Secret extension for TLS versions ≤ 1.2. Non-compliant with NIST guidelines

**EC_POINT_FORMAT EXTENSION**

The server supports the EC_POINT_FORMAT TLS extension. Good configuration
**Test For Industry Best-Practices**

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNSCAA</strong></td>
<td>Information</td>
<td>This domain does not have a Certification Authority Authorization (CAA) record.</td>
<td></td>
</tr>
<tr>
<td><strong>CERTIFICATES DO NOT PROVIDE EV</strong></td>
<td>Information</td>
<td>The RSA certificate provided is NOT an Extended Validation (EV) certificate.</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER DOES NOT SUPPORT OF TLSV1.3</strong></td>
<td>Misconfiguration or weakness</td>
<td>The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER DOES NOT HAVE CIPHER PREFERENCE</strong></td>
<td>Misconfiguration or weakness</td>
<td>The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected.</td>
<td></td>
</tr>
<tr>
<td><strong>ALWAYS-ON SSL</strong></td>
<td>Good configuration</td>
<td>The HTTP version of the website redirects to the HTTPS version.</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER PROVIDES HSTS WITH LONG DURATION</strong></td>
<td>Good configuration</td>
<td>The server provides HTTP Strict Transport Security for more than 6 months: 63072000 seconds</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION</strong></td>
<td>Good configuration</td>
<td>The server does not support client-initiated secure renegotiation.</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER-INITIATED SECURE RENEGOTIATION</strong></td>
<td>Good configuration</td>
<td>The server supports secure server-initiated renegotiation.</td>
<td></td>
</tr>
<tr>
<td><strong>SERVER DOES NOT SUPPORT TLS COMPRESSION</strong></td>
<td>Good configuration</td>
<td>TLS compression is not supported by the server.</td>
<td></td>
</tr>
</tbody>
</table>