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

Summary of editorial.ucatolica.edu.co:443 (HTTPS)

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

RSA CERTIFICATE INFORMATION

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Let's Encrypt Authority X3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>Yes</td>
</tr>
<tr>
<td>Common Name</td>
<td>editorial.ucatolica.edu.co</td>
</tr>
<tr>
<td>Key Type/Size</td>
<td>RSA 2048 bits</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>Subject Alternative Names</td>
<td>DNS:editorial.ucatolica.edu.co</td>
</tr>
<tr>
<td>Transparency</td>
<td>Yes</td>
</tr>
<tr>
<td>Validation Level</td>
<td>DV</td>
</tr>
<tr>
<td>CRL</td>
<td>No</td>
</tr>
<tr>
<td>OCSP</td>
<td><a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a></td>
</tr>
<tr>
<td>OCSP Must-Staple</td>
<td>No</td>
</tr>
<tr>
<td>Supports OCSP Stapling</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid From</td>
<td>May 13th 2020, 02:23 CEST</td>
</tr>
<tr>
<td>Valid To</td>
<td>August 11th 2020, 02:23 CEST</td>
</tr>
</tbody>
</table>

CERTIFICATE CHAIN

DST Root CA X3

<table>
<thead>
<tr>
<th>Key Type/Size</th>
<th>RSA 2048 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>sha1WithRSAEncryption</td>
</tr>
<tr>
<td>SHA256</td>
<td>0687260331a72403d909f105e69bcf0d32e1bd2493ffcc6d9206d11bcd6770739</td>
</tr>
<tr>
<td>PIN</td>
<td>Vjs8r4z+80wjNcr1YKeWQboSIri63WsWXhlMN+eWys=</td>
</tr>
<tr>
<td>Expires in</td>
<td>483 days</td>
</tr>
</tbody>
</table>

Let's Encrypt Authority X3

<table>
<thead>
<tr>
<th>Key Type/Size</th>
<th>RSA 2048 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>SHA256</td>
<td>25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d</td>
</tr>
<tr>
<td>PIN</td>
<td>YLh1dUR9y6KjA30RrAn7JKnBQG/uEtLMkBGF2Fuihg=</td>
</tr>
<tr>
<td>Expires in</td>
<td>286 days</td>
</tr>
</tbody>
</table>

editorial.ucatolica.edu.co

<table>
<thead>
<tr>
<th>Key Type/Size</th>
<th>RSA 2048 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>sha256WithRSAEncryption</td>
</tr>
</tbody>
</table>
SHA256: 808041f445b6a0f54acdb2a064cc5ca6d21476e2d59f820e9c3b19be2f8a6305
PIN: YEfTCtsHHsG6EjBfj+KDrTKz+MF40yLvWSi9w8A5pYc=
Expires in: 67 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>Curve</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>secp256k1 (256 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>P-384 (secp384r1) (384 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>P-521 (secp521r1) (521 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>P-256 (prime256v1) (256 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>K-283 (sect283k1) (281 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>B-283 (sect283r1) (282 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>K-409 (sect409k1) (407 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>B-409 (sect409r1) (409 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>K-571 (sect571k1) (570 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>B-571 (sect571r1) (570 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>brainpoolP256r1 (256 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>brainpoolP384r1 (384 bits)</td>
<td>Good</td>
</tr>
<tr>
<td>brainpoolP512r1 (512 bits)</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

<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 configuration</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

**Diffie-Hellman Parameter Size**

Diffie-Hellman parameter size: 2048 bits

Good configuration

**Supported Elliptic Curves**

List of all elliptic curves supported by the server:

- secp256k1 (256 bits)
- P-384 (secp384r1) (384 bits)
- P-521 (secp521r1) (521 bits)
- P-256 (prime256v1) (256 bits)
- K-283 (sect283k1) (281 bits)
- B-283 (sect283r1) (282 bits)
- K-409 (sect409k1) (407 bits)
- B-409 (sect409r1) (409 bits)
- K-571 (sect571k1) (570 bits)
- B-571 (sect571r1) (570 bits)
- brainpoolP256r1 (256 bits)

Good configuration
Good configuration

brainpoolP384r1 (384 bits)

brainpoolP512r1 (512 bits)

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.
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:

- secp256k1 (256 bits)  
  *Good configuration*
- P-384 (secp384r1) (384 bits)  
  *Good configuration*
- P-521 (secp521r1) (521 bits)  
  *Good configuration*
- P-256 (prime256v1) (256 bits)  
  *Good configuration*
- K-283 (sect283k1) (281 bits)  
  *Good configuration*
- B-283 (sect283r1) (282 bits)  
  *Good configuration*
- K-409 (sect409k1) (407 bits)  
  *Good configuration*
- B-409 (sect409r1) (409 bits)  
  *Good configuration*
- K-571 (sect571k1) (570 bits)  
  *Good configuration*
- B-571 (sect571r1) (570 bits)  
  *Good configuration*
- brainpoolP256r1 (256 bits)  
  *Good configuration*
Good configuration

brainpoolP384r1 (384 bits)

brainpoolP512r1 (512 bits)

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.

SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET
The server does not support Extended Master Secret extension for TLS versions ≤ 1.2.

EC_POINT_FORMAT EXTENSION
The server supports the EC_POINT_FORMAT TLS extension.

Test For Industry Best-Practices

DNSCAA
This domain does not have a Certification Authority Authorization (CAA) record.

CERTIFICATES DO NOT PROVIDE EV
The RSA certificate provided is NOT an Extended Validation (EV) certificate.

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.

SERVER DOES NOT HAVE CIPHER PREFERENCE
The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected.

ALWAYS-ON SSL
The HTTP version of the website redirects to the HTTPS version.

SERVER PROVIDES HSTS WITH LONG DURATION
The server provides HTTP Strict Transport Security for more than 6 months:
63072000 seconds

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION
The server does not support client-initiated secure renegotiation.

SERVER-INITIATED SECURE RENEGOTIATION
The server supports secure server-initiated renegotiation.

SERVER DOES NOT SUPPORT TLS COMPRESSION
TLS compression is not supported by the server.