Summary of gotethics.whistleblowernetwork.net SSL/TLS Security Test

FINAL GRADE

A+

COMPLIANT WITH

PCI DSS

HOST

SERVER IP : PORT
87.116.16.91:443

DATE OF TEST
May 16th 2017, 14:09 CEST

The server configuration seems to be good, but is not entirely compliant with NIST guidelines and HIPAA guidance. Information

The server prefers cipher suites supporting Perfect-Forward-Secrecy. Good configuration

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	DigiCert SHA2 Secure Server CA
Trusted	Yes
Common Name	*.whistleblowernetwork.net
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.whistleblowernetwork.net, DNS:whistleblowernetwork.net
Transparency	No
Validation Level	No
CRL	http://crl3.digicert.com/ssca-sha2-g2.crl
OCSP	http://ocsp.digicert.com
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	June 13th 2014, 02:00 CEST
Valid To	September 13th 2017, 14:00 CEST

CERTIFICATE CHAIN

Server certificate	*.whistleblowernetwork.net
Type/Size	RSA 2048 bits
Signature	sha256WithRSAEncryption
SHA256	d472784a4ef300a92ce51f3...b4d1b2d1c1aab9cd51ea29e
PIN	ZTKqo/w6SF/1NaGy82W65QUMPgKD4NzjYgKmkLG31Dc=
Expires in	120 days
Comment	-

Intermediate CA	DigiCert SHA2 Secure Server CA
Type/Size	RSA 2048 bits
Signature	sha256WithRSAEncryption
SHA256	6edb4a81fe4f8f9a18de803...c5ce3832cbdce4468bd31f3
PIN	5kJvNEMw0KjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=
Expires in	2,122 days
Comment	-

Root CA	DigiCert Global Root CA
Type/Size	RSA 2048 bits
Signature	sha1WithRSAEncryption
SHA256	cbeea2a34b6c7b2c7df9ae0...9352614a46fd816461a30a5
PIN	r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E=
Expires in	5,290 days
Comment	Self-signed

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.2 - Requirements 2.3 and 4.1

CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSv1.2

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration

TLSv1.1

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

TLSv1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.0	Deprecated. Dropped in June 2018
TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration

POODLE OVER TLS

The server's response to invalid TLS packet is not compliant with RFC4346 (section 6.2.3.2) and may be an indicator that the server is vulnerable to POODLE over TLS.

Information

CVE-2016-2107

The server may be vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107), make sure that your OpenSSL version is up to date.

Information

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation.

Good configuration

HEARTBLEED

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

Not vulnerable

CVE-2014-0224

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).

Not vulnerable

Test For Compliance With HIPAA

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

X509 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:

TLSv1.0	Good configuration
TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSv1.2

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration

TLSv1.1

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

TLSv1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration

TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with HIPAA guidance.

Good configuration

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports elliptic curves but not the EC_POINT_FORMAT TLS extension.

Non-compliant with HIPAA guidance

Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 1 - Section 3

X509 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_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration

TLSv1.1

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

TLSv1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.0	Good configuration
TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration

TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with NIST guidelines. Good configuration

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses. Good configuration

EC_POINT_FORMAT EXTENSION

The server supports elliptic curves but not the EC_POINT_FORMAT TLS extension. Non-compliant with NIST guidelines

Test For Industry Best-Practices

DNSCAA

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

Information

CERTIFICATES HAVE BEEN SIGNED FOR MORE THAN 3 YEARS

The RSA certificate provided has been validated for more than 3 years. This means that the private key of the server will remain the same for more than 3 years. NIST guidelines suggest limiting certificate validity to 3 years maximum.

Misconfiguration or weakness

CERTIFICATES DO NOT PROVIDE EV

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

Information

SERVER HAS CIPHER PREFERENCE

The server enforces cipher suites preference.

Good configuration

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration

SERVER PREFERS CIPHER SUITES PROVIDING PFS

For TLS family of protocols, the server prefers cipher suite(s) providing Perfect Forward Secrecy (PFS).

Good configuration

ALWAYS-ON SSL

The HTTP version of the website redirects to the HTTPS version.

Good configuration

SERVER DOES NOT PROVIDE HSTS

The server does not enforce HTTP Strict Transport Security. We advise to enable it to enforce the user to browse the website in HTTPS.

Misconfiguration or weakness

SERVER DOES NOT PROVIDE HPKP

The server does not enforce HTTP Public Key Pinning that helps preventing man-in-the-middle attacks.

Information

TLS_FALLBACK_SCSV

TLS_FALLBACK_SCSV extension prevents protocol downgrade attacks. We advise to update your TLS engine to support it.

Misconfiguration or weakness

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation.

Good configuration

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration