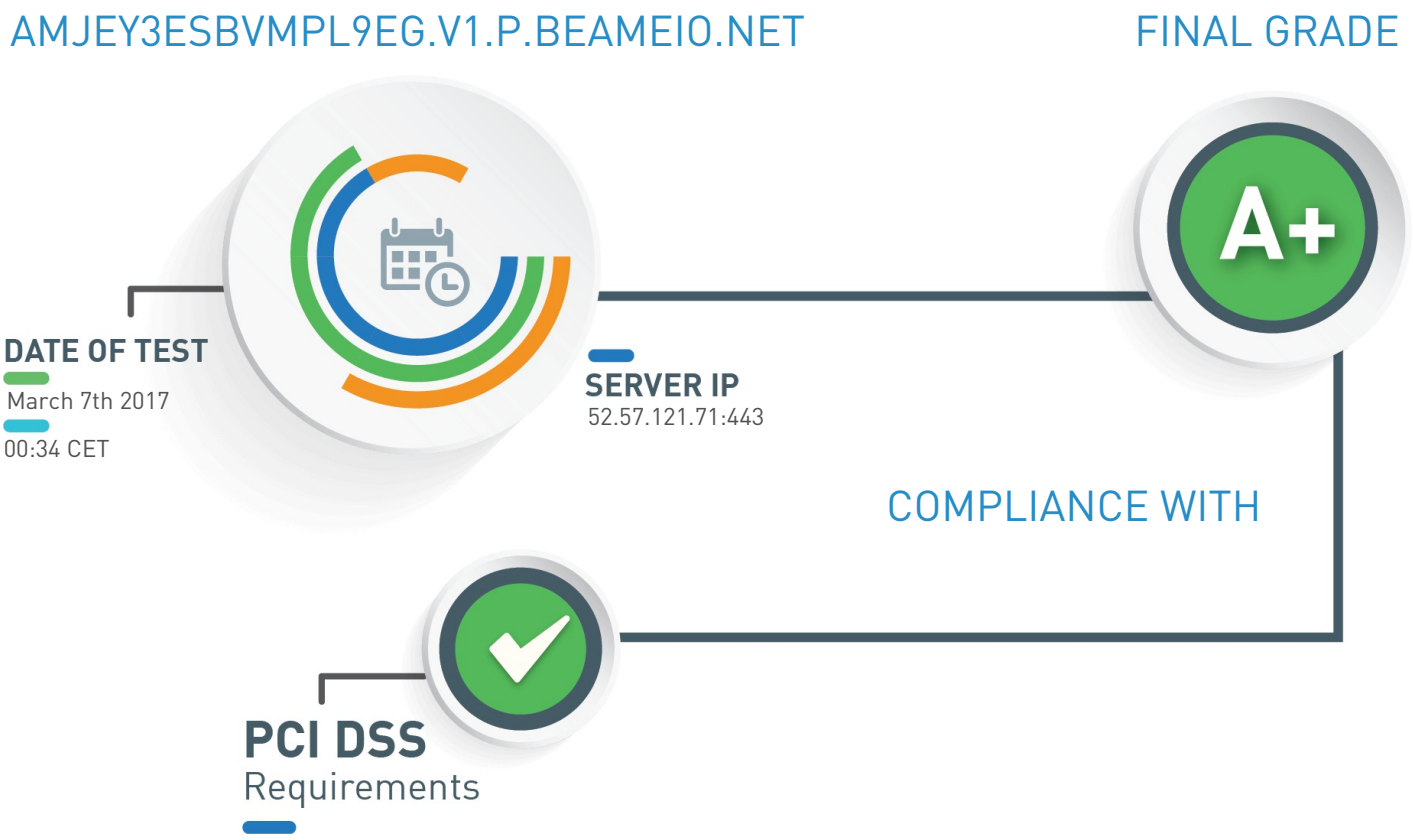
SSL Server Security Test of amjey3esbvmpl9eg.v1.p.beameio.net

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



Assessment Executive Summary

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 Overview

RSA CERTIFICATE INFORMATION

Trusted	Yes
Common Name	amjey3esbvmpl9eg.v1.p.beameio.net
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:amjey3esbvmpl9eg.v1.p.beameio.net
Transparency	No
Extended Validation	No
CRL	No
OCSP	http://ocsp.globalsign.com/ca/beameioca1
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	March 6th 2017, 14:36 CET
Valid To	March 6th 2018, 14:36 CET

CERTIFICATE CHAIN

Server sends an unnecessary root certificate. Misconfiguration or weakness

amjey3esbvmpl9eg.v1.p.beameio.net

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	45c19383977705a3049180408365a050bae93bea59196d7a82722151d5ccf36b
PIN	RYlLCuE3MqeD5lN/xZHcJ7RTKRPyUXQPyfRoYf0M1XU=
Expires in	365 days

Beame.io CA 1

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	2ede44f6018db9de8c44fdb625cfc55d1f5acf992c2e1601671f84f30bf8b229
PIN	5fxJ002g5Il0LSaAZtiEC7BeF8z+cxBoMLk7llE9WeI=
Expires in	1,596 days

Trusted Root CA SHA256 G2

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	0176070032bd2aad1dd44b838d42fdda701908895fbf143871d5d749253510f1
PIN	HHWscHR+mXReMKBRZxCvqEg6wDv6HAbPzKN7NlLvq4c=
Expires in	3,701 days

GlobalSign

Self-signed Root CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	3d0440e1a3e0ad841f123246ce52640602282ce227e09fc69d8494aa63050848
PIN	cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A=
Expires in	4,394 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. 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_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_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_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration

TLSV1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_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-256 (prime256v1) (256 bits)	Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS.

Not vulnerable

CVE-2016-2107

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

Not vulnerable

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 DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status. Non-compliant with HIPAA guidance

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_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_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_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration

TLSV1.0

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

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

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

MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to HIPAA guidance:

TLSV1.1

TLS_RSA_WITH_3DES_EDE_CBC_SHA — Non-compliant with HIPAA guidance

TLSV1.0

TLS_RSA_WITH_3DES_EDE_CBC_SHA — Non-compliant with HIPAA guidance

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 1 - Section 3

X509 CERTIFICATES ARE IN VERSION 3

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

SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling for its RSA certificate. Its support allows better verification of the certificate validation status. Non-compliant with NIST guidelines

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_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_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration

TLSV1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_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-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

MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to NIST guidelines:

TLSV1.1

TLS_RSA_WITH_3DES_EDE_CBC_SHA — Non-compliant with NIST guidelines

TLSV1.0

TLS_RSA_WITH_3DES_EDE_CBC_SHA — 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

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_128_GCM_SHA256	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

HTTP SITE DOES NOT REDIRECT

The HTTP version of the website does not redirect to the HTTPS version. We advise to enable redirection. Misconfiguration or weakness

TLS_FALLBACK_SCSV

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention. Good configuration

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