TLS Audit Report

Server security audit

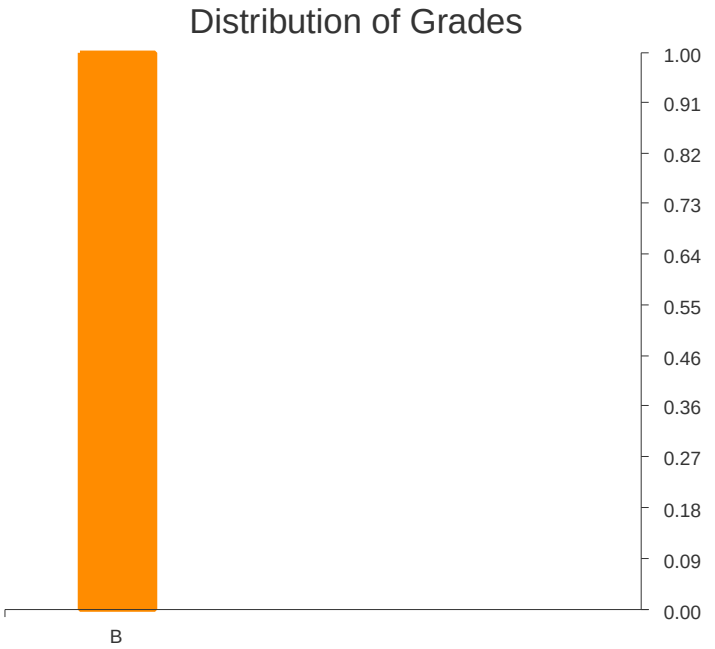
https://github.com/adedayo/tlsaudit v0.0.0

Tue, 14 Apr 2020 22:46:39 UTC

1. Executive Summary

This is a report of the security audit of your server(s) conducted on Tue, 14 Apr 2020 22:46:39 UTC

Worst Measured Grade



Interpretation of Worst Measured Grade

- Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems
- An example is a service running on Port 443 and IP Address 104.154.89.105 with hostname ecc384.badssl.com

Table 1. Grade Legend and count of occurrence

Grade	Meaning	Number Found
B	Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems	1

2. Detailed Metrics

The following are some details and result metrics from the TLS Audit.

Table 2. TLS Audit Metrics

Worst Grade observed	B (on 104.154.89.105:443)
Best Grade observed	B (on 104.154.89.105:443)
Total Number of Hosts (IPs)	1
Total number of Ports (Unique IP:Port(s))	1
IP:Port(s) with grade B	104.154.89.105:443
Grade range for 104.154.89.105	**Worst Grade**: B, **Best Grade**: B

3. Details of Individual Scan Results

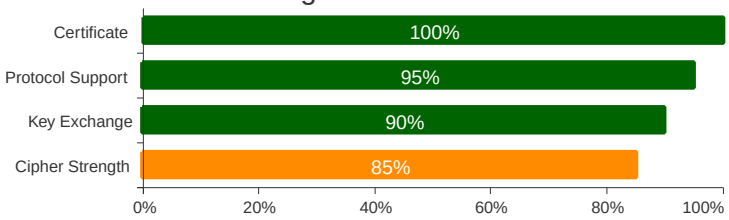
The following sections contain detailed description of results for each port that implements SSL/TLS

TLS Audit Report for 104.154.89.105 (ecc384.badssl.com) on Port 443

Summary

Overall Grade

Rating Breakdown



Advisories

- Grade B : *Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems*
- Supports TLS v1.1 or TLS v1.0. Grade capped to or below B

Certificate number #1: ECDSA EC 384 bits (ECDSA-SHA384)

Server Key and Certificate #1

Subject	CN=*.badssl.com,O=Lucas Garron Torres,L=Walnut Creek,ST=California,C=US
Subject Serial Number	
Common Names	*.badssl.com
Alternative Names	*.badssl.com, badssl.com
Serial Number	b635b2243f89cf86181511051b6adb0
Valid From	Wed, 05 Feb 2020 00:00:00 UTC
Valid Until	Thu, 10 Feb 2022 12:00:00 UTC
Key Algorithm	ECDSA
Key	EC 384 bits
Issuer	CN=DigiCert ECC Secure Server CA,O=DigiCert Inc,C=US
Signature Algorithm	ECDSA-SHA384
Signature	3066023100a3e6d0…9dfc597ff97ee46c
OCSP Must Staple	false
Certificate Version	3
Chain Length	2
Has Chain Issues	false Chain 1 (CA: false): CN=*.badssl.com,O=Lucas Garron Torres,L=Walnut Creek,ST=California,C=US. (Expires: Thu, 10 Feb 2022 12:00:00 UTC) Chain 0 (CA: true): CN=DigiCert ECC Secure Server CA,O=DigiCert Inc,C=US. (Expires: Wed, 08 Mar 2023 12:00:00 UTC)

Configuration

Supported Protocols

TLS v1.2
TLS v1.1
TLS v1.0

Cipher Suites

TLS v1.2 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) (Supported Group: secp256r1) FS	128	A
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) (Supported Group: secp256r1) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) (Supported Group: secp256r1) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) (Supported Group: secp256r1) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) (Supported Group: secp256r1) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) (Supported Group: secp256r1) FS Weak	112	A

TLS v1.1 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) (Supported Group: secp256r1) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) (Supported Group: secp256r1) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) (Supported Group: secp256r1) FS Weak	112	A

TLS v1.0 (suites in server-preferred order)

	Supports secure renegotiation: true

	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) (Supported Group: secp256r1) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) (Supported Group: secp256r1) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) (Supported Group: secp256r1) FS Weak	112	A