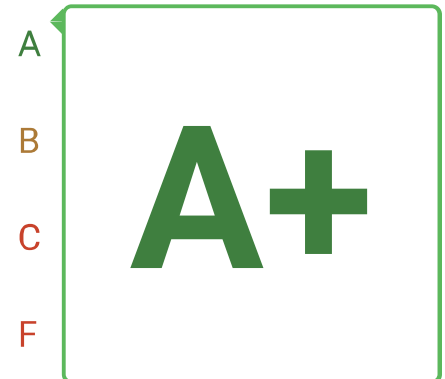



# Summary of audit.coretechnologies.com:443 (HTTPS) SSL Security Test

coretechnologies.com was tested 2 times during the last 12 months.

## Your final score



Date/Time: Sep 4th, 2023 18:55:23 GMT-7  
Source IP/Port: 98.210.29.70:443   
Type: HTTPS

  
Compliance Test  
**COMPLIANT**

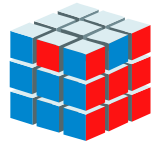
  
Compliance Test  
**NO MAJOR ISSUES FOUND**

  
Compliance Test  
**NO MAJOR ISSUES FOUND**

  
Industry Best Practices  
**NO MAJOR ISSUES FOUND**

  
External Content Security  
**NOT FOUND**

The server supports the most recent and secure TLS protocol version of TLS 1.3. **Good configuration**



**ImmuniWeb<sup>®</sup>**  
AI for Application Security

## Upgrade from Free Community Edition to ImmuniWeb<sup>®</sup> AI Platform Now!



[API Penetration Testing](#)



[Mobile Penetration Testing](#)



[API Security Scanning](#)



[Mobile Security Scanning](#)



[Attack Surface Management](#)



[Network Security Assessment](#)



[Cloud Penetration Testing](#)



[PCI DSS Penetration Testing](#)



[Cloud Security Posture Management](#)



[Phishing Websites Takedown](#)



[Continuous Penetration Testing](#)



[Red Teaming Exercise](#)



[Cyber Threat Intelligence](#)



[Software Composition Analysis](#)



[Dark Web Monitoring](#)



[Third-Party Risk Management](#)



[Digital Brand Protection](#)



[Web Penetration Testing](#)



[GDPR Penetration Testing](#)



[Web Security Scanning](#)

[Free Demo](#)

[Book a Call](#)

# Discovered Subdomains

No subdomains were found.


Information

# SSL Certificate Analysis


## RSA CERTIFICATE INFORMATION

<b>Issuer</b>	GoGetSSL RSA DV CA
<b>Trusted</b>	Yes
<b>Common Name</b>	audit.coretechnologies.com
<b>Key Type/Size</b>	RSA 2048 bits
<b>Serial Number</b>	0xF7C63734F619116565FDEE8E01390447
<b>Signature Algorithm</b>	sha256WithRSAEncryption
<b>Subject Alternative Names</b>	DNS:audit.coretechnologies.com, DNS:www.audit.coretechnologies.com
<b>Transparency</b>	Yes
<b>Validation Level</b>	DV
<b>CRL</b>	http://crl.usertrust.com/GoGetSSLRSADVCA.crl
<b>OCSP</b>	http://ocsp.usertrust.com
<b>OCSP Must-Staple</b>	No
<b>Supports OCSP Stapling</b>	No
<b>Valid From</b>	September 04, 2023 01:00 CET
<b>Valid To</b>	December 04, 2023 00:59 CET

## CERTIFICATE CHAIN

 Root CA	<b>AAA Certificate Services</b>
<b>Type/Size</b>	RSA 2048 bits
<b>Serial Number</b>	1
<b>Signature</b>	sha1WithRSAEncryption
<b>SHA256</b>	7a7a0fb5d7e2731d77...782bc83ee0ea699ef4
<b>PIN</b>	vRU+17BDT2iGsXvOi7...LXAqj0+jGPdW7L1vM=
<b>Expires in</b>	1,945 days
<b>Comment</b>	Self-signed

 Intermediate CA	<b>USERTrust RSA Certification Authority</b>
<b>Type/Size</b>	RSA 4096 bits

**Serial Number** 76359301477803385872276235234032301461  
**Signature** sha384WithRSAEncryption  
**SHA256** 68b9c761219a5b1f01...ca9f74244ee5f5f52b  
**PIN** x4QzPSC810K5/cMjb0...5zBn4ITdO/nEW/Td4=  
**Expires in** 1,945 days

**Comment** -

 Intermediate CA **GoGetSSL RSA DV CA**

**Type/Size** RSA 2048 bits  
**Serial Number** 0x938BB08E62987B4F75F98CB6A5045C96  
**Signature** sha384WithRSAEncryption  
**SHA256** 43cac31ef8e8ba1b4b...e90170e41b66c2fd64  
**PIN** T+6uyT5C6WT480t2wq...t2j8v52bWLj+Xlvz8=  
**Expires in** 1,828 days

**Comment** -

 Server certificate **audit.coretechnologies.com**

**Type/Size** RSA 2048 bits  
**Serial Number** 0xF7C63734F619116565FDEE8E01390447  
**Signature** sha256WithRSAEncryption  
**SHA256** 0164739c211617d373...dcd0bd0b27e03e1cad  
**PIN** iW4sX0hXe8IZMZuRX1...49VO1JuKgloUn/8vc=  
**Expires in** 90 days

**Comment** -

 Root CA **USERTrust RSA Certification Authority**

**Type/Size** RSA 4096 bits  
**Serial Number** 2645093764781058787591871645665788717  
**Signature** sha384WithRSAEncryption  
**SHA256** e793c9b02fd8aa13e2...64b1746d46c3d4cbd2  
**PIN** x4QzPSC810K5/cMjb0...5zBn4ITdO/nEW/Td4=  
**Expires in** 5,250 days

**Comment** Self-signed

# PCI DSS Compliance Test

Reference: [PCI DSS 3.2.1](#), 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:

### TLSV1.3

TLS\_CHACHA20\_POLY1305\_SHA256

Good configuration

TLS\_AES\_256\_GCM\_SHA384

Good configuration

TLS\_AES\_128\_GCM\_SHA256

Good configuration

### TLSV1.2

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Good configuration

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

Good configuration

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Good configuration

TLS\_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\_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

TLSv1.3

Good configuration

## SUPPORTED ELLIPTIC CURVES

---

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-256 (prime256v1) (256 bits)

Good configuration

X25519 (253 bits)

Good configuration

X448 (448 bits)

Good configuration

## POODLE OVER TLS

---

The server is not vulnerable to POODLE over TLS.

Not vulnerable

## GOLDENDOODLE

---

The server is not vulnerable to GOLDENDOODLE.

Not vulnerable

## ZOMBIE POODLE

---

The server is not vulnerable to Zombie POODLE.

Not vulnerable

## SLEEPING POODLE

---

The server is not vulnerable to Sleeping POODLE.

Not vulnerable

## 0-LENGTH OPENSSL

---

The server is not vulnerable 0-Length OpenSSL.

Not vulnerable

## CVE-2016-2107

---

The server is not vulnerable to CVE-2016-2107.

Not vulnerable

## SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

---

The server does not support client-initiated insecure renegotiation.

Good configuration

## ROBOT

---

The server is not vulnerable to ROBOT vulnerability.

Not vulnerable

## HEARTBLEED

---

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

Not vulnerable

#### **CVE-2014-0224**

---

The server is not vulnerable to CCS Injection.

**Not vulnerable**

#### **CVE-2021-3449**

---

The server is not vulnerable to CVE-2021-3449 (OpenSSL Maliciously Crafted Renegotiation Vulnerability).

**Not vulnerable**



# HIPAA and NIST Compliance Test

Reference: [HIPAA](#), Security Rule (Ref. [NIST SP 800-52](#): "Guidelines for the Selection and Use of TLS Implementations")

## X.509 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 is not configured to support OCSP stapling for its RSA certificate that allows better verification of the certificate validation status. [Reconfigure or upgrade](#) your web server to enable OCSP stapling.

Non-compliant with NIST guidelines

## SUPPORTED CIPHERS

List of all cipher suites supported by the server:

### TLSV1.3

TLS\_CHACHA20\_POLY1305\_SHA256

Good configuration

TLS\_AES\_256\_GCM\_SHA384

Good configuration

TLS\_AES\_128\_GCM\_SHA256

Good configuration

### TLSV1.2

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Good configuration

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

Good configuration

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Good configuration

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

Good configuration

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Good configuration

TLS\_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\_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

TLSv1.3

Good configuration

## SUPPORTED ELLIPTIC CURVES

---

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-256 (prime256v1) (256 bits)

Good configuration

X25519 (253 bits)

Good configuration

X448 (448 bits)

Good configuration

## SERVER DOES NOT SUPPORT SERVER NAME INDICATION

---

The server does not support [Server Name Indication \(SNI\)](#) extension for TLS versions  $\leq 1.3$ . SNI allows a user to specify the domain name it's trying to connect to, and prevents common name mismatch errors, when a server hosts several domains with different SSL certificates.

Information

## EC\_POINT\_FORMAT EXTENSION

---

The server supports the EC\_POINT\_FORMAT TLS extension.

Good configuration

# Industry Best Practices Test

## DNSCAA

---

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

Information

## CERTIFICATES DO NOT PROVIDE EV

---

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

Information

## TLSV1.3 SUPPORTED

---

The server supports TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Good configuration

## 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.

Misconfiguration or weakness

## SERVER PREFERRED CIPHER SUITES

---

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

## 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

## 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

## 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**

# External Content Privacy and Security Analysis

No external content found on tested page.

Information