Symantec.CryptoReport

Check your SSL/TLS certificate installation

Pick a tool

Do you nee

www.oldvic

www.old

This is not a Syr
Please contact th

Info

BEAST
This server

Certificate inf

This server
Data is pro

Common name
SAN: oldvicarage
cpanel.oldvicara
mail.oldvicarage
webdisk.oldvicar
webmail.oldvicar
www.oldvicarage

Valid from: 201
Valid to: 2018-Ju

Certificate statu
Revocation che

Certificate cha

COM
Inter

Certificate chain details

COMODO RSA Certification Authority (Intermediate certificate)

Certificate information

Common name: COMODO RSA Certification Authority
SAN:

Valid from: 2000-May-30 10:48:38 GMT
Valid to: 2020-May-30 10:48:38 GMT

Organization: COMODO CA Limited
Organizational unit:
City/locality: Salford
State/province: Greater Manchester
Country: GB
Certificate Transparency: Not embedded in certificate

Serial number: 2766ee56eb49f38eabd770a2fc84de22
Algorithm type: SHA384withRSA
Key size: 4096

cPanel, Inc. Certification Authority (Intermediate certificate)

Certificate information

Common name: cPanel, Inc. Certification Authority
SAN:

Valid from: 2015-May-18 00:00:00 GMT
Valid to: 2025-May-17 23:59:59 GMT

Certificate status: Valid
Revocation check method: OCSP

Organization: cPanel, Inc.
Organizational unit:
City/locality: Houston
State/province: TX
Country: US
Certificate Transparency: Not embedded in certificate

Serial number: f01d4bee7b7ca37b3c0566ac05972458
Algorithm type: SHA384withRSA
Key size: 2048

oldvicaragepenzance.co.uk (Tested certificate)

Certificate information

Common name: oldvicaragepenzance.co.uk
SAN: oldvicaragepenzance.co.uk, cpanel.oldvicaragepenzance.co.uk, mail.oldvicaragepenzance.co.uk, webdisk.oldvicaragepenzance.co.uk, webmail.oldvicaragepenzance.co.uk, www.oldvicaragepenzance.co.uk

Valid from: 2018-Apr-18 00:00:00 GMT
Valid to: 2018-Jul-17 23:59:59 GMT

Certificate status: Valid
Revocation check method: OCSP

Organization:
Organizational unit:
City/locality:
State/province:
Country:
Certificate Transparency: Embedded in certificate

Serial number: 437e2212854b0a81ff7de2d3cd8261f5
Algorithm type: SHA256withRSA
Key size: 2048

Symantec.CryptoReport

Check your SSL/TLS certificate installation

Do you need another certificate? Compare SSL/TLS Certificates.

TLS1.0

Protocols not enabled:
SSLv3
SSLv2

Vulnerabilities checked:
Heartbleed
Poodle (TLS)
Poodle (SSLv3)
FREAK
BEAST
CRIME

RC4: Not Enabled
OCSP stapling: Enabled

Cipher suites enabled:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009E)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009F)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xC012)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)