

TECHNICAL REPORT



Passive Security Audit *for Web Applications*

The Acme Corporation Ltd.



2020 September, 7

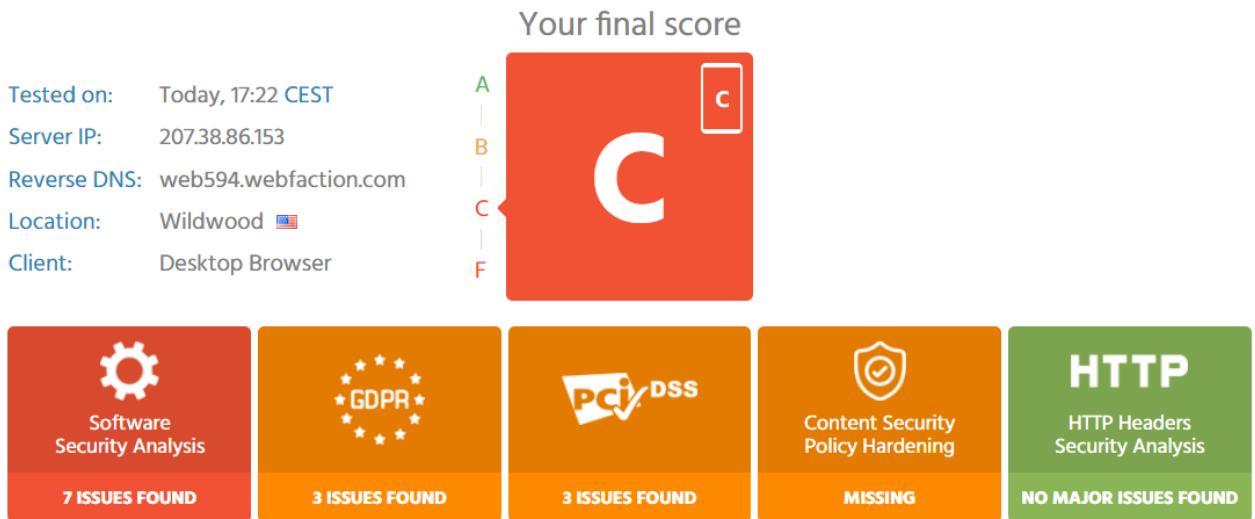
Gianandrea Daverio
Cybersecurity & Compliance Manager

M +39 342 9928782

E gianandrea.daverio@nposistemi.it

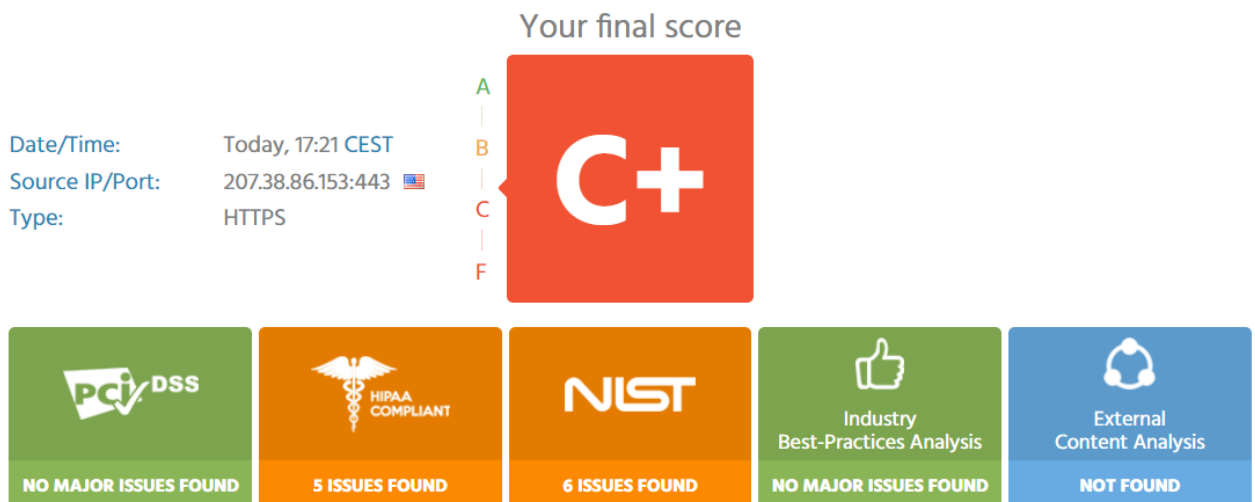
Web Application Security Test

Summary of theacmecorporation.org [Desktop Version] Website Security Test



Secure Socket Layer Security Test

Summary of theacmecorporation.org:443 (HTTPS) SSL Security Test



Web Application

PASSIVE SECURITY AUDIT

Summary of theacmecorporation.org [Desktop Version] Website Security Test

FINAL GRADE



DNS

SERVER IP

207.38.86.153

REVERSE DNS

web594.webfaction.com

CLIENT

Desktop Browser

INFO

DATE OF TEST

October 8th 2020, 17:22

SERVER LOCATION

Wildwood

Web Server Security

HTTP RESPONSE

200 OK

REDIRECT TO

N/A

NPN

N/A

ALPN

N/A

CONTENT ENCODING

None

SERVER SIGNATURE

nginx

WAF

No WAF detected

LOCATION

server4you Inc.

HTTP METHODS ENABLED

GET POST HEAD OPTIONS

Software Security Analysis

A non-intrusive CMS fingerprinting technology thoroughly crawls some parts of the CMS to fingerprint its version in the most accurate manner:

FINGERPRINTED CMS & VULNERABILITIES

No CMS were fingerprinted on the website.

[Information](#)

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 1.11.1

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.5.1**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2020-11022	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 — Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 — Prototype pollution
4.2 Medium	CVE-2020-11023	CWE-79 — Cross-site scripting

Datatables 1.10.6

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **1.10.20**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.3 Medium	CVE-2015-6584	CWE-79 — Cross-site scripting

Twitter-bootstrap 3.3.4

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **4.5.1**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2016-10735	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14040	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14042	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14041	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2019-8331	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20677	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20676	CWE-79 — Cross-site scripting

Html5shiv 3.7.0

The component is outdated. No known security vulnerabilities found. Update to the most recent version **3.7.3**.

JQuery Easing Plugin 1.3

The component is outdated. No known security vulnerabilities found. Update to the most recent version **1.4.1**.

Classie 1.0.0

The component is outdated. No known security vulnerabilities found. Update to the most recent version **1.0.1**.

JqBootstrapValidation 1.3.6

The component is outdated. No known security vulnerabilities found. Update to the most recent version **1.3.8**.

Animated-header 0.0.1

The fingerprinted component version is up2date, no security issues were found.

GDPR Compliance Analysis

If the website processes or stores any PII of EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY

Privacy Policy was not found on the website or is not easily accessible.

Misconfiguration or weakness

WEBSITE SOFTWARE SECURITY

Website CMS or its components are outdated and contain known security vulnerabilities.

Misconfiguration or weakness

SSL/TLS TRAFFIC ENCRYPTION

SSL/TLS encryption is missing or insecure.

Misconfiguration or weakness

COOKIE CONFIGURATION

No cookies with potentially sensitive information seem to be sent.

Information

COOKIES DISCLAIMER

No cookies with potentially sensitive or tracking information seem to be sent.

Information

PCI DSS Compliance Analysis

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.2

Website CMS or its components seem to be outdated. Check for available updates.

Misconfiguration or weakness

REQUIREMENT 6.5

Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10).

Misconfiguration or weakness

REQUIREMENT 6.6

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.

Misconfiguration or weakness

HTTP Headers Security Analysis

Some HTTP headers related to security and privacy are missing or misconfigured.

Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

X-Frame-Options X-XSS-Protection X-Content-Type-Options Expect-CT

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin Permissions-Policy

SERVER

Web server does not disclose its version.

Good configuration

Raw HTTP Header

Server: nginx

Content Security Policy Hardening

CONTENT-SECURITY-POLICY

The header was not sent by the server.

Misconfiguration or weakness

Cookies Security Analysis

No cookies were sent by the web application.

[Information](#)

Secure Socket Layer

PASSIVE SECURITY AUDIT

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



Summary of theacmecorporation.org:443 (HTTPS)

The server's certificate is untrusted.

Non-compliant with PCI DSS requirements

The server has TLS 1.1 enabled. NIST recommends to drop TLS 1.1 support since SP 800-52 REV. 2

Information

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	Go Daddy Secure Certificate Authority - G2
Trusted	No
Untrusted Reasons	The certificate doesn't match hostname
Common Name	*.webfaction.com
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.webfaction.com, DNS:webfaction.com
Transparency	Yes
Validation Level	DV
CRL	http://crl.godaddy.com/gdig2s1-1588.crl
OCSP	http://ocsp.godaddy.com/
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	December 18th 2019, 22:02 CET
Valid To	December 18th 2021, 22:02 CET

CERTIFICATE CHAIN

Server sends an unnecessary root certificate.

Misconfiguration or weakness

Go Daddy Root Certificate Authority - G2

Self-signed

Root CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	45140b3247eb9cc8c5b4f0d7b53091f73292089e6e5a63e2749dd3aca9198eda
PIN	Ko8tivDrEjiY90yGasP6ZpBU4jwXvHqVvQI0GS3GNdA=
Expires in	6,293 days

Go Daddy Secure Certificate Authority - G2

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	973a41276ffd01e027a2aad49e34c37846d3e976ff6a620b6712e33832041aa6
PIN	8Rw90Ej3Tt8RRkrG+WYDS9n7IS03bk5bjP/UXPtaY8=
Expires in	3,859 days

↳ *.webfaction.com

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	8e9db539d4ba06de383177d31bb5dbcd21a62db965dd8c4eaf4a3023c6090a0c
PIN	MfumKLN/e83oeROHIC9dySAhAl4fLrW3e/qJmfmPnUY=
Expires in	436 days

PCI DSS Compliance Analysis

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

CERTIFICATES ARE UNTRUSTED

The RSA certificate provided by the server could not be trusted.

Non-compliant with PCI DSS requirements

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_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_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_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_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_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_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Good configuration

TLS_RSA_WITH_AES_128_CBC_SHA

Good configuration

TLS_RSA_WITH_AES_256_CBC_SHA

Good configuration

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

Good configuration

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Good configuration

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

Good configuration

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.1

Good configuration

TLSv1.2

Good configuration

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-384 (secp384r1) (384 bits)

Good configuration

secp256k1 (256 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 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

ROBOT

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) 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 CVE-2014-0224 (OpenSSL CCS flaw).

Not vulnerable

HIPAA Compliance Analysis

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

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 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:

- TLSv1.1 Good configuration
- TLSv1.2 Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA Good configuration
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Good configuration
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA Good configuration
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA Good configuration
- TLS_RSA_WITH_AES_128_CBC_SHA Good configuration
- TLS_RSA_WITH_AES_256_CBC_SHA Good configuration
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA Non-compliant with HIPAA guidance
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA Non-compliant with HIPAA guidance
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA Non-compliant with HIPAA guidance
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA Non-compliant with HIPAA guidance
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Good configuration
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Good configuration
- TLS_DHE_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_DHE_RSA_WITH_AES_128_CBC_SHA256 Good configuration
- TLS_DHE_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_RSA_WITH_AES_128_CBC_SHA256

Good configuration

TLS_RSA_WITH_AES_256_CBC_SHA256

Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Good configuration

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Good configuration

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Good configuration

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Good configuration

TLS_RSA_WITH_AES_128_CBC_SHA

Good configuration

TLS_RSA_WITH_AES_256_CBC_SHA

Good configuration

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

Non-compliant with HIPAA guidance

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Non-compliant with HIPAA guidance

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

Non-compliant with HIPAA guidance

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

Non-compliant with HIPAA guidance

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits

Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)

Good configuration

P-521 (secp521r1) (521 bits)

Good configuration

P-384 (secp384r1) (384 bits)

Good configuration

secp256k1 (256 bits)

Good configuration

TLSV1.1 SUPPORTED

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

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

NIST Compliance Analysis

Reference: NIST Special Publication 800-52 Revision 2 - Section 3

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 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_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_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_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_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_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
------------------------------------	--------------------

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines

SUPPORTED PROTOCOLS

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

TLSv1.1	Good configuration
TLSv1.2	Good configuration

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits	Good configuration
--	--------------------

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
secp256k1 (256 bits)	Good configuration

TLSV1.1 SUPPORTED

The server supports TLSv1.1. It's still compliant, but NIST recommends to drop TLS 1.1 support since SP 800-52 REV. 2	Information
---	-------------

SERVER DOES NOT SUPPORT OF TLSV1.3

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.	Information
---	-------------

SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET

The server does not support Extended Master Secret extension for TLS vresions ≤ 1.2.	Non-compliant with NIST guidelines
--	------------------------------------

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.	Good configuration
--	--------------------

Industry Best Practices Analysis

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

SERVER DOES NOT SUPPORT OF TLSV1.3

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

Misconfiguration or weakness

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:

TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	

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

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.

Cybersecurity portfolio

CYBER SECURITY Operations		
SECURE DIGITAL Business	SECURE DIGITAL Identity	SECURE Industrial IoT
SECURE Hybrid Cloud		
SECURE DIGITAL Infrastructure		
SECURE DIGITAL Workplace		
Consulting Services		
Managed Services		

Web Application Security offering

<p>BREACH & ATTACK SIMULATION</p> <p>Web Application Breach & Attack Simulation</p> 	<p>VULNERABILITY ASSESSMENT</p> <p>Web Application Vulnerability Assessment</p> <p>CMS & API Vulnerability Assessment</p> 	<p>IDENTITY & ACCESS MANAGEMENT</p> <p>User Provisioning & Lifecycle Management</p> <p>Risk-based Adaptive Authentication</p> 	<p>WEB APPLICATION SECURITY GATEWAY</p> <p>Web Application Firewall</p> <p>DDoS Prevention</p> 
--	--	--	---

NPO SISTEMI S.R.L.

Viale Martesana, 12 20090 Vimodrone (MI)

Telefono: +39 02 925961 - Fax: +39 02 92590092

Sede Legale: Via Vittor Pisani, 6 - 20124 Milano (MI)

P.IVA e C.F. 08820850967 - Cap.Soc. € 2.100.284,00 i.v.

Filiale di Torino

Lungo Dora Colletta 81 10153 Torino

Tel. +39 011 19701225

Filiale di Roma

Via Mario Bianchini, 15 00142 Roma

Tel. +39 06 837881.1

Agenzia di Padova

Via Medoaco 2 (via Po) 35135 Padova

Tel. +39 049 865 0862