

Security and limitations

To ensure security Apptimized complies with the following cybersecurity standards:

- ISO 15408;
- ISO/IEC 27001;
- ISO/IEC 27002;
- ANSI/ISA 62443 (Formerly ISA-99);
- IEC 62443;

A military-grade security protocol (TLS/SSL) is used by Apptimized to provide privacy and data integrity between two or more communicating applications.

Apptimized safety audit entails a network scan of its resources to identify vulnerabilities and non-penetration.

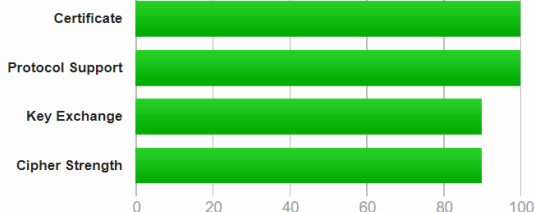
The screenshot below shows the vulnerability report provided by **Detectify** for **app.apptimized.com**.

The screenshot displays a vulnerability report generated by Detectify for the target **app.apptimized.com**. The report is structured into three main panels:

- Summary Panel (Left):** Features the Detectify logo and the title "VULNERABILITY REPORT app.apptimized.com". It includes scan timestamps: "Scan Started 2020-02-25T00:06:00+00:00" and "Scan Finished 2020-02-25T00:25:58+00:00".
- 1.1 Fingerprinted Software Panel (Middle):** Contains a "Summary" section with the target "Found at app.apptimized.com" and a "CVSS Score 0". It also lists "References" such as "DETECTIFY - An intelligent way to look for vulnerabilities" and "DETECTIFY - What's under the hood". Below this, a list of fingerprinted software is shown, including Microsoft Windows (Confidence: 30), Microsoft Internet Information Services (IIS) 10.0 (Confidence: 100), Microsoft ASP.NET Core (Confidence: 50), Intel Active Management Technology (Confidence: 50), and Sharp (Confidence: 50).
- Findings Panel (Right):** Titled "Findings" with a link to "All findings summary". It displays a risk scale with categories: HIGH (No findings), MEDIUM (No findings), LOW (No findings), and INFORMATION. A list of findings is provided at the bottom, including "Fingerprinted Software", "Strict-Transport-Security / Missing Header", "Discovered Host", "Crawled URL's", "Service Providers", and "Recorded User Events Failed using app.apptimized.com-recording-1920x937".

The screenshots below show the SSL report of **app.apptimized.com**.

[Scan Another »](#)



This site works only in browsers with SNI support.

[illegible]

NSA	FS	WEAK	
NSA	FS	WEAK	ECJH weq25dr1 (wq. 30/2 bits)
1LS	NSA WITH AES	256	GCM SHA256 (dr0d) WEAK 120
1LS	NSA WITH AES	128	GCM SHA256 (dr0c) WEAK 120
1LS	NSA WITH AES	256	CBC SHA256 (dr1d) WEAK 120
1LS	NSA WITH AES	128	CBC SHA256 (dr1c) WEAK 120
1LS	NSA WITH AES	256	CBC SHA (dr2d) WEAK 120
1LS	NSA WITH AES	128	CBC SHA (dr2c) WEAK 120

[illegible]

Header	no
BEAST attack	Microsoft servers only (more info)
POODLE (SSLv2)	No (SSL 3 not supported)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 (no-ssl2)
GOLOUSEK attack	No (more info) TLS 1.2 (no-ssl2)
OpenSSL 0-Length	No (more info) TLS 1.2 (no-ssl2)
Streaming POODLE	No (more info) TLS 1.2 (no-ssl2)
Downgrade attack	Unknown (requires support for at least two protocols, see SSL2)
SSL/TLS compression	No
RC4	No
Heartbleed (extension)	No (more info)
Heartbleed (vulnerability)	No (more info)
Logjam (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2016-2122)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2121)	No (more info)
ROCCO (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) HIGHEST (more info)
AUTH	Yes (all major)
NRN	No
Session resumption (seamless)	No (CIE assigned but not accepted)
Session resumption (ticket)	No
OCSP	No
Strict Transport Security (STS)	No
OCSP Stapling	No
MD-5 Pseudo	Not in: Chrome, Edge, Firefox, IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning (HPKP) Only	No (more info)
Public Key Pinning (Static)	No
Long handshake tolerance	No
TLS extension intolerance	No
TLS session intolerance	No
Incomplete DT alerts	No
Use common DH primes	No, DHF suites not supported
DH public server param	No, DHF suites not supported
TLS reuse	No
ECDF public server param	No
Reuse	No
Suggested Named Groups	ssl2DHE1, ssl2DHE1 (server preferred)
SSL 2 handshake compatibility	No

SSL Report v2.1.0

Copyright © 2009-2020 Quipix, Inc. All Rights Reserved

Try Qualys for free! Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including certificate security solutions.

Tertre and

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempted successful. Browsers sometimes rely with a slower protocol version.

(4) Detects a reference browser or client, with which we expect better effective success.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS

Protocol Details	
OSI Layer	Application
Port	80, 443
Protocol	<p>No, server keys and hostname not used elsewhere with SSLv2 (1) or a better understanding of that field, please read the original specification</p> <p>Yes, the protocol is widely provided by the Census network search engine, original L2VPN website here</p> <p>(2) Census data is only available through key and certificate names, probably out-of-date but not complete</p>
Secure Negotiation	Supported
Secure Client-Initiated Negotiation	No
Insecure Client-Initiated Negotiation	No
BR/AS Attack	Mitigated server-side (more info)

The SCCM connector must be launched on a local PC by the domain administrator or domain user.

Domain user must have the permissions to:

- create applications, deployment types, and deployments;
- write permissions for network share with packages source media for automatic media transfer.

Revision #3

Created 4 March 2020 12:29:30

Updated 29 March 2022 06:55:47