

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.

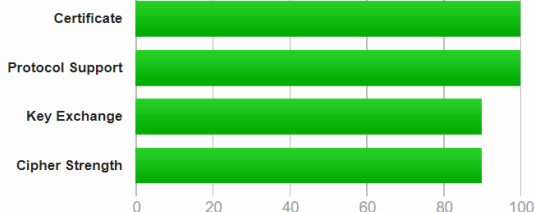
The screenshot below shows the vulnerability report provided by **Detectify** for **app.apptimized.com**.

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, the title "VULNERABILITY REPORT" for **app.apptimized.com**, and 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 "Found at app.apptimized.com" and a "CVSS Score 0". It includes a "References" section with links to Detectify blog posts. Below this is a list of fingerprinted software items, each with vendor, software name, version, and confidence level:
 - Vendor: microsoft, Software: windows, Confidence: 30
 - Vendor: microsoft, Software: is, Version: 10.0, Confidence: 100
 - Vendor: microsoft, Software: asp_net_core, Confidence: 50
 - Vendor: microsoft, Software: iisexpress, Confidence: 50
 - Vendor: microsoft, Software: csharp, Confidence: 50
- Findings Panel (Right):** Titled "Findings" with a link to "All findings summary". It shows four severity levels: HIGH, MEDIUM, LOW, and INFORMATION. The HIGH, MEDIUM, and LOW sections all report "No findings". The INFORMATION section lists six items:
 - 1 Fingerprinted Software
 - 2 Strict-Transport-Security / Missing Header
 - 1 Discovered Host
 - 1 Created URL's
 - 1 Service Providers
 - 1 Recorded User Events Failed using app.apptimized.com-recording-1920x937

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

[Scan Another »](#)



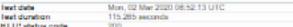
This site works only in browsers with SNI support.

[illegible]

NSA	FS	WEAK				
NSA	FS	WEAK	ECB, EDE, DES, WITH AES, 128, CBC, SHA (RecB1)	ECB, wesp256b1 (wsp. 30/2 bits)		120
115	NSA WITH AES	256	GCM	SHA384 (b60d)	WEAK	120
115	NSA WITH AES	128	GCM	SHA256 (b6b)	WEAK	120
115	NSA WITH AES	256	CBC	SHA256 (b6b)	WEAK	120
115	NSA WITH AES	128	CBC	SHA256 (b6b)	WEAK	120
115	NSA WITH AES	256	CBC	SHA (b6b)	WEAK	120
115	NSA WITH AES	128	CBC	SHA (b6b)	WEAK	120

[illegible]

Header	Value
HeaderNegotiation	Merged server-side (more info)
BEAST1 attack	No, SSL 3 not supported (more info)
POODLE (SSLv2)	No (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2: Dec027
GOLDENPOODLE	No (more info) TLS 1.2: Dec027
OpenSSL 0-Length	No (more info) TLS 1.2: Dec027
Sleeping POODLE	No (more info) TLS 1.2: Dec027

[illegible]

SSS Report v2.1.0

Downloaded from <http://ajph.org/> on November 10, 2015

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

Tertro and

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

(2) No support for virtual SSL, loading (SNI). Connects to the default id of the server once SNI is supported.

(3) Only first connection attempt simulated. Servers sometimes reply with a lower protocol version.

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

(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 handhelds 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 here and includes 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