

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:** 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:** Contains a "Summary" section with "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, several software fingerprints are listed with their vendors, software names, versions, and confidence levels (e.g., "Vendor: microsoft, Software: windows, Confidence: 30").
- Findings Panel:** Titled "Findings" with a link to "All findings summary". It shows a breakdown of findings by severity: "HIGH" (No findings), "MEDIUM" (No findings), "LOW" (No findings), and "INFORMATION" (6 items). The information items include "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**.


Feature	Percentage
Certificate	100%
Protocol Support	98%
Key Exchange	88%
Cipher Strength	88%

This site works only in browsers with SNI support.


Cipher Suites	
# TLS 1.2 (available in server-on-demand mode)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x0307) ECDH sec256r1 eq. 307/2	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0304) ECDH sec256r1 eq. 307/2	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0x0309) ECDH sec256r1 eq. 307/2	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0x0306) ECDH sec256r1 eq. 307/2	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x0307) ECDH sec256r1 eq. 307/2	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0304) ECDH sec256r1 eq. 307/2	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0x0309) ECDH sec256r1 eq. 307/2	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0306) ECDH sec256r1 eq. 307/2	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x0307) ECDH sec256r1 eq. 307/2	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0304) ECDH sec256r1 eq. 307/2	128

[illegible]

OpenSSL version:	Unknown (requires support for at least two protocols, vnd. SSL2)
OpenSSL TLS compression:	No
RC4:	No
Heartbleed (vulnerability):	No
Heartbleed (vulnerability):	No (more info)
Indefinite (vulnerability):	No
OpenSSL CVEs (CVE-2014-0224):	No (more info)
OpenSSL (Pending Oracle CVEs):	No
(CVE-2016-2107):	No (more info)
ROBUST (vulnerability):	No (more info)
Forward Secrecy:	Yes (with more browsers)
ALPN:	Yes (to http 1.1)
NPN:	No
Session resumption (cookies):	No (N/A assigned but not accepted)
Session resumption (tickets):	No
CCSP (logging):	No
Strict Transport Security (STS1.0):	No
HTTPS (Preloading):	Not in Chrome, Edge, Firefox, IE
Public Key Pinning (HPKP):	No (more info)
Public Key Pinning Report-Only:	No
Public Key Pinning (Strict):	No (more info)
Long Handshake intolerance:	No
TLS extension intolerance:	No
TLS version intolerance:	No
Incorrect SSL alerts:	No
Uses compression (Dh prime):	No, DHc, suites not supported
Use public server param:	No, DHc, suites not supported
(Tls) reuse:	No
ECDF (public server param reuse):	yes256r1, yes256r1 (server provided order)
Supported Named Groups:	SSL 2 handshake
SSL 2 handshake:	No


 https://app.appformid.com/ (HTTPIV1.1 302 Found)

1 https://app.appformid.com/Account/Login?ReturnUrl=%2F (HTTPIV1.1 200 OK)


 Welcome

Last date Mon, 02 Mar 2020 08:52:13 UTC

Last duration 11s, 263s seconds

IP 191.17.174.100

IP 191.17.174.100

Kunal

SSL Report v2.1.0

Copyright © 2009-2020 Quipva, 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.

Errors and

Conclusion

Protocol Details	
DROWN	No, server keys and handshake not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this bugzilla entry
Secure Negotiation	Not supported (only provided by the Cyrus network search engine; original DROWN database here)
Secure Client-Initiated Negotiation	Supported
Insecure Client-Initiated Negotiation	No
BRACE 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