Bitwarden Network Security Assessment Report

ISSUE SUMMARIES, IMPACT ANALYSIS, AND RESOLUTION

BITWARDEN, INC

June 29th, 2021

Table of Contents

Summary

In June, 2021, Bitwarden hired security firm Insight Risk Consulting to evaluate the security of the Bitwarden network perimeter as well as penetration testing and vulnerability assessments against Bitwarden web services and applications. The scope of this assessment included the Bitwarden product website, web vault application, and backend server systems that power our applications such as the APIs, database, and hosting infrastructure.

During the tests performed by the Insight Risk Consulting team, no exploitable vulnerabilities were discovered and three issues of moderate severity were highlighted. These results are very positive, especially given the extensive size and complexity of Bitwarden's overall infrastructure.

This report was prepared by the Bitwarden team to cover the scope of the identified issues, how they affect the Bitwarden platform and its users, and what steps (if any) have been taken (or are planned) to resolve the issues. For completeness, a copy of the executive summary delivered by Insight Risk Consulting has also been attached to this report.

Issues

Issue-01 – Minimum Accepted TLS Version Too Low for Icons Service

Bitwarden operates an icon server at icons.bitwarden.net that is used to display user-friendly icon images related to the website being stored next to login items in the vault listing. Cloudflare, our proxy service, was configured with a default minimum TLS version value of 1.0.

Impact

Certain devices could connect to the icon service using TLS version 1.0, which has the possibility of introducing cryptographic design flaws.

Resolution

Cloudflare, our proxy service, has been configured to require TLS 1.2 as the minimum accepted version on the entire *.bitwarden.net domain.

Issue-02 – Outdated jQuery Code Library

The Bitwarden product website (bitwarden.com) utilizes jQuery as a third-party JavaScript library that enables key functionality. The version of jQuery being utilized was 3.4.1, which has known vulnerabilities that have been patched in more recent versions.

Impact

After evaluating our use of jQuery, it was determined that we were not subject to any exploitation of the vulnerabilities known in jQuery 3.4.1.

Resolution

As is customary with third-party library maintenance, the jQuery library was updated to the latest version at the time, version 3.6.0.

Issue-03 – CORS Misconfigurations on Third-Party JavaScript Libraries

Several misconfigurations of CORS headers were detected on third-party libraries that are referenced by the Bitwarden product website and help documentation (bitwarden.com).

Impact

CORS header misconfigurations on domains hosting third-party libraries referenced by our website does not impose any security issues.

Resolution

CORS header configurations on third-party domains are considered out of scope for this exercise. This issue required no action and has been deemed to be a false-positive from the scanning tools used during this assessment.

This page was intentionally left blank

Insight
Risk Consulting

June 29, 2021

Mr. Michael Crandell, CEO
Bitwarden Inc.
1 N. Calle Cesar Chavez, Suite 102
Santa Barbara CA 93103

Dear Mr. Crandell:

Insight Risk Consulting has completed an External Network Penetration Test and Vulnerability Assessment of Bitwarden Inc. for the timeframe of June 7 to June 11, 2021.

We evaluated the security of the service provider's systems by simulating an attack by a person with malicious intent. Unlike an information security audit, which is based on external standards, a penetration test is of variable scope with the aim of compromising a target in any way possible via selective targeting.

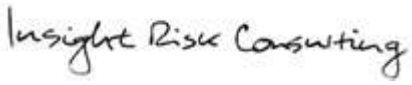
The scope of this test was as follows:

1. External vulnerability assessment of the service provider's in scope systems
2. External penetration testing of the service provider's in scope systems

This report is for the exclusive use of the service provider's management and directors and is not intended for public distribution. However, it may be provided to your external accountants and regulatory agencies.

Please call Jeremy Taylor with any questions about this report. Insight Risk Consulting would like to thank the service provider's management and staff for the cooperation and support received throughout this engagement.

Sincerely,



Insight Risk Consulting

Southern California 6131 Orangethorpe Ave, #470 Buena Park, CA 90620 Tel: 562.802.3581 Fax: 562.683.0399
Northern California PO Box 641148 San Jose, CA 95164 Tel: 408.980.8099 Fax: 408.715.2529

www.insightriskconsulting.com