Bitwarden Network Security Assessment Report

ISSUE SUMMARIES, IMPACT ANALYSIS, AND RESOLUTION

BITWARDEN, INC

July 17th, 2020

Table of Contents

Summary

In June, 2020, 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 two 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 – CORS Configuration Allows Any Origin

The Cross Origin Resource Sharing (CORS) configuration on Bitwarden server APIs allows for any client origin to access its endpoints.

Impact

A web application hosted at any origin is permitted to call into the Bitwarden server APIs. This could allow for a malicious website (for example, in a phishing attack) to use Bitwarden server APIs to appear legitimate.

Resolution

Since legitimate origins are well known, a whitelist has been configured on Bitwarden server APIs to allow only the Bitwarden web vault application to have unrestricted access. Namely, the `Access-Control-Allow-Origin` header will always return the web vault origin (for example, https://vault.bitwarden.com or a self-hosted server's host URL).

ISSUE-02 – Content Security Policy Allows “style-src unsafe-inline”

The Content Security Policy (CSP) configuration on the Bitwarden web vault application allows for `'unsafe-inline'` CSS styles to execute.

Impact

If a Cross Site Scripting (XSS) vulnerability were to be exploitable, it might be possible for a malicious script to change the CSS styling on the Bitwarden web vault application. Maliciously changing the web vault application styling could potentially be used to trick users into performing certain actions that they normally would not. However, the risk of this type of attack occurring is currently mitigated by the fact that the existing Content Security Policy is well-tuned to protect against Cross Site Scripting attacks.

Resolution

It is considered best practice to only execute CSS styling from hosted `.css` files, however, a few third-party libraries that are used in the web vault application require the ability to perform inline-styling. In addition to the existing Content Security Policy that is in place to protect against Cross Site Scripting attacks, we will investigate replacements for these third-party libraries so that in the future the web vault application’s Content Security Policy can be further tuned to deny inline-styling with `style-src 'self'`.

This page was intentionally left blank

Insight
Risk Consulting

July 1, 2020

Bitwarden Inc.
1 N Calle Cesar Chavez, Suite 102
Santa Barbara, CA, 93103

Insight Risk Consulting has completed an External Penetration Test and Vulnerability Assessment of Bitwarden Inc. for the timeframe of June 8 to June 13, 2020. Results were reviewed with Bitwarden management on June 19, 2020.

We evaluated the security of the Bitwarden Internet perimeter, informational website, and web application 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 Bitwarden computing systems and web applications
2. External penetration testing of the Bitwarden computing systems and web applications

Insight Risk Consulting would like to thank Bitwarden management and staff for the cooperation and support received throughout this engagement.

Insight Risk Consulting

Insight Risk Consulting

EXECUTIVE SUMMARY

The test focused on all web applications, computing systems, and devices attached to the Internet perimeter. Emphasis was placed on finding vulnerabilities in accessible web applications, routers, switches, firewalls, servers and other hosts. Potential targets identified during the discovery and enumeration process were later tested for vulnerabilities. Attempts were made to exploit potential vulnerabilities to gain access to various systems.

These tests were carried out from the perspective of a potential attacker using grey hat hacking methodologies. However, please note that these vulnerabilities do not explicitly consider the likelihood of an actual attack. Therefore, the risk ratings as used in this report may overstate the actual risks, since they do not consider probability or frequency of such attacks. While high-risk vulnerabilities deserve management's attention, prioritization of remediation efforts should also take into account the likelihood of these scenarios.

Test	Results
External Penetration Test	Using the information we gathered during the reconnaissance and scanning stage on all the external networks, websites, and web applications, we were unable to identify any vulnerabilities which we could exploit.
External Vulnerability Assessment	The Bitwarden Vault Web Application was built with due consideration of security concerns. We did not identify any critical or high-risk vulnerabilities associated with its Vault Web Application, API library, Community Forums, informational website, or other web assets that support these sites. In addition, we observed that strong TLS encryption is used when customers are accessing these assets. We identified two moderate-priority enhancements to improve the Bitwarden Vault Web Application: 1. We recommend reviewing Cross Origin Resource Sharing (CORS) configuration on a small number of files to determine whether further enhancement is needed. 2. While we observed that the Bitwarden Vault has strong Content Security Policy (CSP) in place, we recommend a minor enhancement to one of its policy settings. We also identified one low-priority enhancement to the CSP on the Community Forums. Management will contact Civilized Discourse Construction Kit, Inc., who developed the Forum application, for further guidance.