CyberTest™

Vulnerability Assessment
&
Penetration Test Report

For Keeper Security

Report Date: July 27, 2023

Legal Notice

This document contains private and confidential information. It is intended for the exclusive use of Keeper Security. Unauthorized use or reproduction of this document is prohibited. Current Test has been conducted by CyberTest security tester(s) and we assure that the findings in this report are true to the extent that can be verified. This Vulnerability Assessment & Penetration Test reveals all relevant vulnerabilities known up to the date of this report.

The information provided in this compression report about password managers is for informational purposes only. While efforts have been made to ensure the accuracy and reliability of the information presented, it should not be construed as legal advice or endorsement of any particular product or service.

The author(s) of this report disclaim any liability, whether direct or indirect, arising from the use or reliance upon the information contained herein. The author(s) shall not be held responsible for any loss, damages, or legal consequences resulting from the use, misuse, or inability to use any password manager mentioned in this report.

Disclosure and Use of the Report

This report contains information concerning potential vulnerabilities of Keeper Security applications, networks, systems and methods of exploiting them. CyberTest recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein. CyberTest has retained and secured a copy of the report for customer reference. All other copies of the report have been delivered to Keeper Security. While CyberTest considers the major security vulnerabilities of the analyzed systems have been identified, there can be no assurance that all possible vulnerabilities can be identified. Nonetheless, CyberTest does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended. This report was prepared by CyberTest (cybertest.com) for the exclusive use and benefit of Keeper Security.

Methodology

Our security assessment methodology is based on both internal and industry best practices, including but not limited to, SANS SWAT, SANS Top 25, OWASP (Open Web Application Security Project) Top 10 and NIST 800-115. Before anything first we conduct reconnaissance to map the application or network. Then we conduct vulnerability assessment and penetration testing using both automated tools and manual attacks to find security gaps and weaknesses. For every finding we provide recommendation how to remediate the finding. Once the test is complete we provide the full report with all the details.

Zero-Knowledge Testing

Keeper uses Zero-Knowledge Architecture which means Keeper has no knowledge or access to master password, keys and data in the vault. Keeper uses master password derived key to encrypt data key locally on user's device. The data key is securely generated locally and is used to encrypt data in Keeper and also to decrypt the vault. All data encryption and decryption is done locally on user's device and Keeper only sends encrypted data to Keeper Cloud. For users who login with SSO Cloud, a locally generated elliptic curve key pair encrypts and decrypts the vault in order to preserve zero knowledge. As part of CyberTest security assessment and penetration testing we look for any violation of zero knowledge. We check and make sure passwords, keys and data are encrypted locally on user's device before it's sent to Keeper Cloud and vice-versa where the decryption is done on user's device.

Tools

Our security team uses many types of tools to do vulnerability assessment and penetration testing. The tools used in performing the services include, but are not limited to: RamDump, FTK, Burp Suite, ZAP, Fiddler, Nmap, SQLMap, WireShark, Postman, OpenSSL, OpenVAS, Acunetix, Nessus, and Proprietary Tools.

Executive Summary

This report presents the results of the vulnerability assessment and penetration test of Keeper Security Windows Desktop App. This assessment was performed under the auspices of CyberTest certified and skilled security tester(s). The purpose of this assessment is to identify application level security issues that could affect Keeper Security's applications, network infrastructure and client sensitive data.

To evaluate the security of biometric key storage in Windows Web Credentials Manger, CyberTest performed penetration testing to determine the overall security by performing a wide variety of vulnerability tests. Both manual pen testing and automated security tools were used for the analysis to increase the thoroughness and the efficiency. The tools that were used in performing the services include, but are not limited to, the following: RamDump, FTK Imager.

The objective of the analysis is to see if biometric key remains in memory and if we can extract the biometric key from Windows Web Credentials Manager from different Windows user account or using program. Every finding includes an overview of issues found and security guidelines, which, if followed correctly, will ensure the confidentiality, integrity and the availability of the systems and applications of Keeper Security.

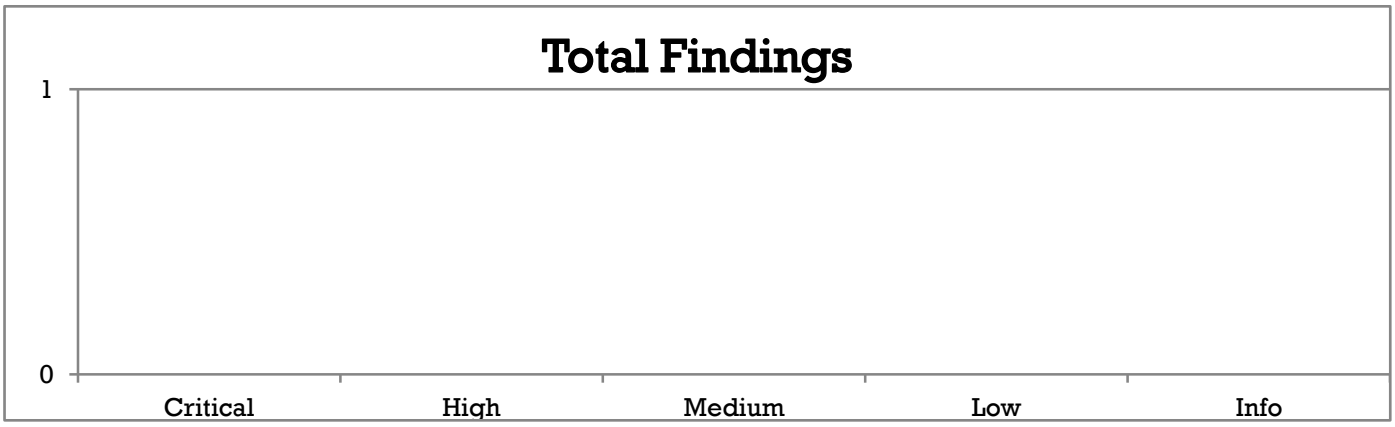
Date Tested: July 26th – 27th 2023

Assets Tested

Name	Type	URL/Domain/IP	Environment	Notes
Keeper Security	Memory check of biometric key	Windows Desktop App 16.10.2	Prod	Using Windows 10 Pro with Windows Hello auth
Keeper Security	Reading biometric key from Windows Web Credentials	Windows Desktop App 16.10.2	Prod	Using Windows 10 Pro with Windows Hello auth

Total Findings

Critical	High	Medium	Low	Info
0	0	0	0	0



Vulnerability Risk Classification

Throughout the document, each vulnerability or risk identified has been labeled as a Finding and it is categorized as Critical, High, Medium, Low or Informational.

C

Critical: These findings identify conditions that could cause extreme damage or directly result in the compromise or unauthorized access of a network, system, application or information. Critical risks must be fixed as soon as possible.

H

High: These findings identify conditions that could cause huge damage or directly result in the compromise or unauthorized access of a network, system, application, device or information. High risks are recommended to get fixed soon after Criticals.

M

Medium: These findings identify conditions that could cause mediocre damage or that not directly or immediately compromise network, system, application, device or information. Medium risks are recommended to get fixed after High risks are addressed.

L

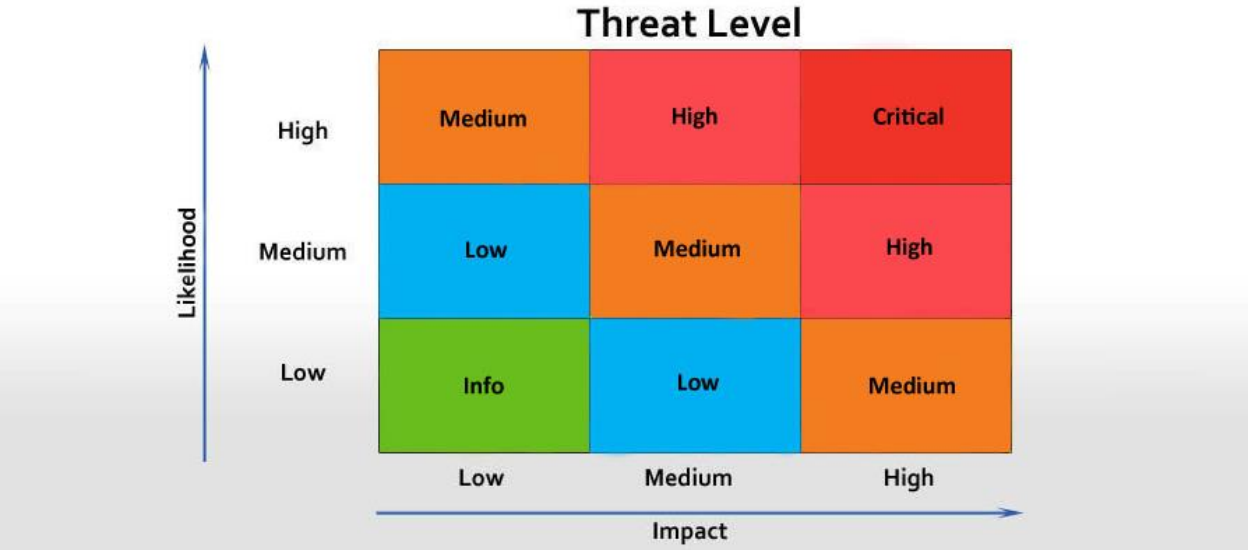
Low: These findings identify conditions that could cause minor damage or that not directly or immediately compromise or unauthorized access of a network, system, application, device or information. Low risks are recommended to get fixed after mediums.

I

Info: These are informational only. No direct threat to confidentiality, integrity or availability of the data, applications, systems or devices. The information can be used for awareness. It can also be used for hardening the security of the asset.

Severity Risk Matrix

CyberTest ranks the severity of the risk using the matrix below. Each threat is measured using impact and likelihood. Combining both impact and likelihood gives the severity risk.



Findings Matrix

The matrix below provides high level summary of security assessment findings ranked by severity. Each finding gives you the issue found and recommendation how to fix it. For detail description of the issue, how to reproduce and screenshots can be found below this matrix. Note that some findings in details below the matrix may be exactly same as in this matrix if there is no extra information.

Item	Issue	Severity	Description	Recommendation	Status
Appendix 1: Comparing with Bitwarden Appendix 2: Comments					

Findings Details

The findings below provides detail level summary of security assessment found in the matrix above. It may contain steps on how to reproduce the vulnerability, screenshots and other more technical information needed to prove the security issue exists.

Appendix 1 – Comparing with other password managers

Bitwarden:

We downloaded Windows Bitwarden latest version to compare with Keeper. We then turned on Hello authentication.
Below you can see the screenshot of where Bitwarden stores the biometric key.

Using a C++ program we can dump Bitwarden password from Windows Credentials.

```
Target Name: LegacyGeneric:target=Bitwarden_biometric/1370f0d9-ccfa-4f69-bcba-b00d01686968_masterkey_biometric_witness
Type: 1
Username: 1370f0d9-ccfa-4f69-bcba-b00d01686968_masterkey_biometric_witness
Password: 0.DyRjXNXI2DN4sbJo0nNYkw==|s73TyAuqrBUPYCy8iUwhFA==
-----------------------------------
Target Name: LegacyGeneric:target=Bitwarden_biometric/1370f0d9-ccfa-4f69-bcba-b00d01686968_masterkey_biometric
Type: 1
Username: 1370f0d9-ccfa-4f69-bcba-b00d01686968_masterkey_biometric
Password: 0.DyRjXNXI2DN4sbJo0nNYkw==|xGuyfvLZdkwEdBthXtEcwBLjTB8UemClg5IfVHKU20YCR0S/Adq72WfPfTIrq1zx
```

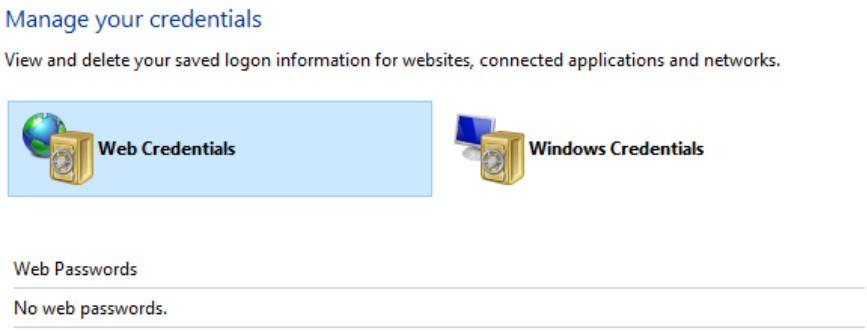
Using python script from CVE-2023-27706 POC outputs:
Biometric master key: d03c918d73572360cde2c6c9a349cd624c

We think the password is encrypted with Windows Hello but note that we have not confirmed that and this was solely just for comparison and not a vulnerability test of Bitwarden application.

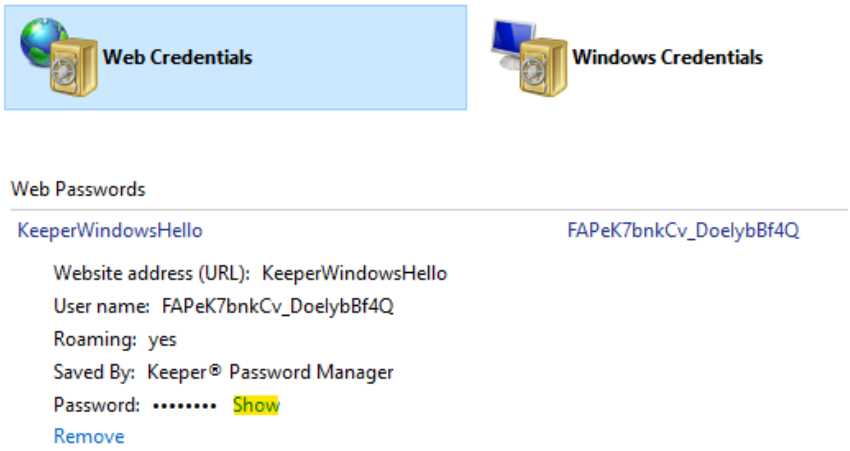
Appendix 2 – Comments

There were no findings testing Keeper Windows Desktop App related to biometric key. Unable to find biometric key in system memory. Also unable to read biometric key from Windows Web Credentials where Keeper stores the key. Logging in as different user does not show up under Web Credentials. Used the POC python script to test the CVE-2023-27706 for Keeper Desktop App but also unable to retrieve the biometric key. From our analysis we determined that Keeper is securely storing and protecting the biometric key using Windows recommended Web Credentials Manager. The credentials are protected by Windows Hello authentication/encryption.

Below shows Windows Web Credentials after logged in as different user. As you can see Keeper biometric key is not there.



However logged in as the user that is using Windows Hello to login to Keeper, you can see the biometric key is stored under Web Credentials Manager.



One recommendation is to see if you can disable or remove the “Show” button from Windows Credentials Manager. This is not a security risk because in order to show the biometric key the user has to get authenticated with Windows Hello. However if we can disable the reveal password from the UI it will be better as an alternative security control.