UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0325

CRITICAL FLAW IN KEEPASS EXPOSES MASTER PASSWORDS IN CLEAR TEXT

DATE ISSUED: 7th June 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

A critical vulnerability in KeePass password manager lets a potential attacker obtain a plaintext master password from a user workspace, even if the workspace is locked. The memory dump can be a KeePass process dump, swap file (pagefile.sys), hibernation file (hiberfil.sys), or RAM dump of the entire system.

BREAKDOWN

Security researcher 'vdohney' disclosed a vulnerability and proof-of-concept exploit that could allow an attacker to partially extract the cleartext KeePass master password from a memory dump of the application. The vulnerability is tracked as CVE-2023-32784 with a CVSS score of 7.5. KeePass is a free, open-source password manager that helps manage passwords and stores them in encrypted form. When a new KeePass password manager database is created, users are asked to create a master password, which is used to encrypt the whole database, i.e., not just the passwords but also usernames, URLs, notes, etc. A master password leak is generally considered the worst-case scenario for a password manager, as the master password can be used to access all logins for accounts stored in a password manager instance. However, Users of KeePass 1.x, Strongbox, or KeePassXC are not impacted by this vulnerability and, thus, do not need to migrate to a newer release. KeePass has released version 2.54, which fixes the vulnerability.

REMEDIATION STEPS

- All users of the 2.x branch are strongly recommended to upgrade to KeePass 2.54 version.
- Users who cannot upgrade to KeePass 2.54 are recommended to reset their master password, delete crash dumps and hibernation files, and swap files that might contain fragments of their master password.
- Turn on device encryption to keep unauthorised users from accessing your system.
- Regularly monitor the network to detect and respond to anomalous network activity.

REFERENCES & RESOURCES

Malwarebytes https://www.malwarebytes.com/blog/news/2023/05/keepass-vulnerability-allows-attackers-to-access-the-master-password

Bleeping Computer https://www.bleepingcomputer.com/news/security/keepass-v254-fixes-bug-that-leaked-cleartext-master-password/