بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

افشای رمز عبور با بهره برداری از آسیب پذیری KeePass

گزارش و تحلیل خبر آسیب پذیری

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۴۰۲/۰۲/۳۰

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ مقدمه

برنامه مدیر رمزعبور[۱]مشهور KeePass در برابر استخراج رمزعبور اصلی از حافظه برنامه آسیب‌پذیر بوده و به مهاجمانی که دستگاه را به خطر می‌اندازند این امکان را می‌دهد تا رمزعبور را حتی با پایگاه‌داده قفل شده بازیابی کنند. این مشکل توسط یک محقق امنیتی معروف به "vdohney" کشف شد که ابزاری را منتشر نمود که با استفاده از اثبات مفهوم[۲]به مهاجمان اجازه می‌دهد تا رمزعبور اصلی KeePass را از حافظه استخراج کنند.

برنامه مدیریت رمزعبور، به کاربران اجازه می‌دهند برای هر حساب آنلاین رمزهای عبور منحصر به فردی ایجاد کنند و اعتبارنامه‌ها را در یک پایگاه‌داده با قابلیت جستجوی آسان ذخیره کنند، بنابراین لازم نیست هر کدام از رمزها را به خاطر بسپارید. با این حال، کاربران برای ایمن سازی مناسب می‌بایست رمزعبور اصلی را که برای باز کردن قفل و دسترسی به اطلاعات کاربری ذخیره شده استفاده می‌شود، به خاطر بسپارند.

این رمز عبور اصلی، پایگاه داده رمز KeePass را رمزنگاری می‌کند و بدون وارد کردن رمزعبور، از باز شدن یا خوانده شدن این پایگاه داده جلوگیری می‌کند. با این حال، هنگامی که رمزعبور اصلی در معرض خطر قرار می‌گیرد، عامل تهدید می‌تواند به تمام اعتبارنامه‌های ذخیره شده در پایگاه داده دسترسی داشته باشد. بنابراین، برای این‌که یک برنامه مدیر رمزعبور به درستی ایمن شود، این نکته که کاربران از رمزعبور اصلی محافظت کنند و آن را با دیگران به اشتراک نگذارند امری بسیار مهم است.

۲ جزئیات آسیب پذیری

آسیب‌پذیری جدید KeePass که با عنوان CVE-2023-3278 پیگیری می‌شود، جدا از یک یا دو کاراکتر اول، بازیابی رمز عبور اصلی KeePass را به فرم متن واضح[۳]و بدون در نظر گرفتن قفل بودن فضای کاری KeePass یا بسته بودن برنامه، ممکن می‌سازد.

محقق امنیتی GitHub در مورد ابزار بهره‌برداری هشدار می‌دهد که: "KeePass Master Password Dumper یک ابزار اثبات مفهوم ساده است که برای تخلیه رمزعبور اصلی از حافظه KeePass استفاده می‌شود. این ابزار، جدا از اولین کاراکتر رمزعبور، بیشتر قادر به بازیابی رمزعبور در متن عادی[۴]است."

---

۱ password manager

۲ اثبات مفهوم (Proof of Concept) نمونه‌ای است که صرفاً برای اثبات وجود یا امکان‌پذیری چیزی آورده می‌شود.

۳ Cleartext یا متن بدون رمز

۴ plaintext

"نیاز به هیچ اجرای کدی در سیستم هدف نیست، فقط یک حافظه تخلیه شده مورد نیاز است. مهم نیست که حافظه از کجا آمده است- می‌تواند **فرآیند dump، فایل مبادله‌ای[۱](pagefile.sys)، فایل hibernation (hiberfil.sys) یا تخلیه RAM[۲]**کل سیستم باشد. **فرقی نمی‌کند که فضای کاری قفل باشد یا نباشد.**"

این نقص به این دلیل وجود دارد که نرم‌افزار از یک جعبه ورود رمز عبور سفارشی به نام "SecureTextBoxEx" استفاده می‌کند. این نرم‌افزار آثار هر کاراکتری را که کاربر تایپ می‌کند، در حافظه باقی می‌گذارد.

vdohney توضیح می‌دهد که: "KeePass 2.X از یک جعبه متنی سفارشی توسعه یافته با نام SecureTextBoxEx، برای ورود رمزعبور استفاده می‌کند. این جعبه متنی نه تنها برای ورود رمزعبور اصلی به کار برده می‌شود، بلکه در قسمت های دیگر KeePass مانند جعبه‌های ویرایش رمزعبور نیز استفاده می‌شود."

این آسیب‌پذیری آخرین نسخه KeePass، یعنی نسخه 2.53.1 را تحت تأثیر قرار می‌دهد و از آن‌جا که این برنامه منبع باز است، هر نسخه‌ای از پروژه نیز احتمالاً تحت تأثیر قرار می‌گیرد.

به گفته توسعه‌دهنده ابزار تخلیه رمزعبور، KeePass 1.X، KeePassXC و Strongbox تحت تأثیر آسیب-پذیری CVE-2023-32784 قرار نگرفته‌اند.

در حالی که فرایند تخلیه رمزعبور اصلی فقط برروی ویندوز آزمایش شد، اما این بهره‌برداری با برخی تغییرات باید برای لینوکس و macOS نیز کار کند، زیرا این مشکل فقط مختص سیستم‌عامل نیست، بلکه مربوط به نحوه مدیریت ورودی کاربر توسط KeePass است.

۳ بهره برداری آسان

از آن‌جا که برای بازیابی رمزعبور اصلی KeePass، حافظه‌های تخلیه شده باید بازیابی شوند، بهره‌برداری از CVE-2023-32784 بر روی دستگاه مورد نظر، نیاز به دسترسی فیزیکی یا آلودگی با استفاده از بدافزار دارد.

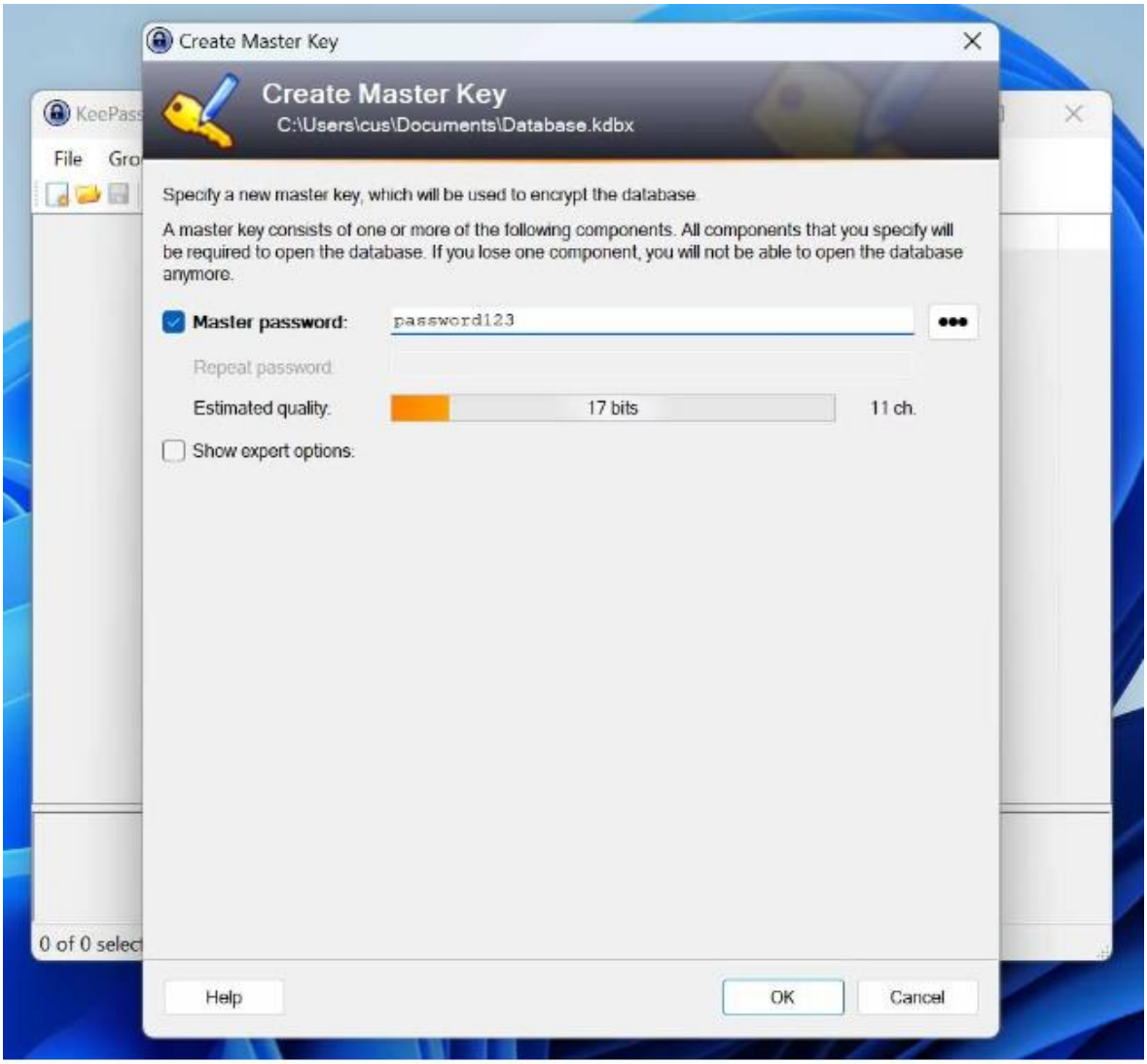
با این حال، بدافزار سرقت اطلاعات می‌تواند به سرعت بررسی کند که آیا KeePass در رایانه هدف وجود دارد یا در حال اجرا است یا خیر و اگر چنین است، حافظه برنامه را تخلیه می‌نماید و آن حافظه و پایگاه‌داده KeePass را برای مهاجم ارسال میکند. هدف از این کار، بازیابی آفلاین رمز عبور متن عادی از حافظه تخلیه شده است.

---

[۱] swap file

[۲] RAM dump

BleepingComputer ابزار keepass-password-dumper را با نصب KeePass بر روی یک دستگاه آزمایشی و ایجاد یک پایگاه‌داده جدید با رمزعبور اصلی 'password123'، همان‌طور که در شکل زیر نشان داده شده است، آزمایش نمود.

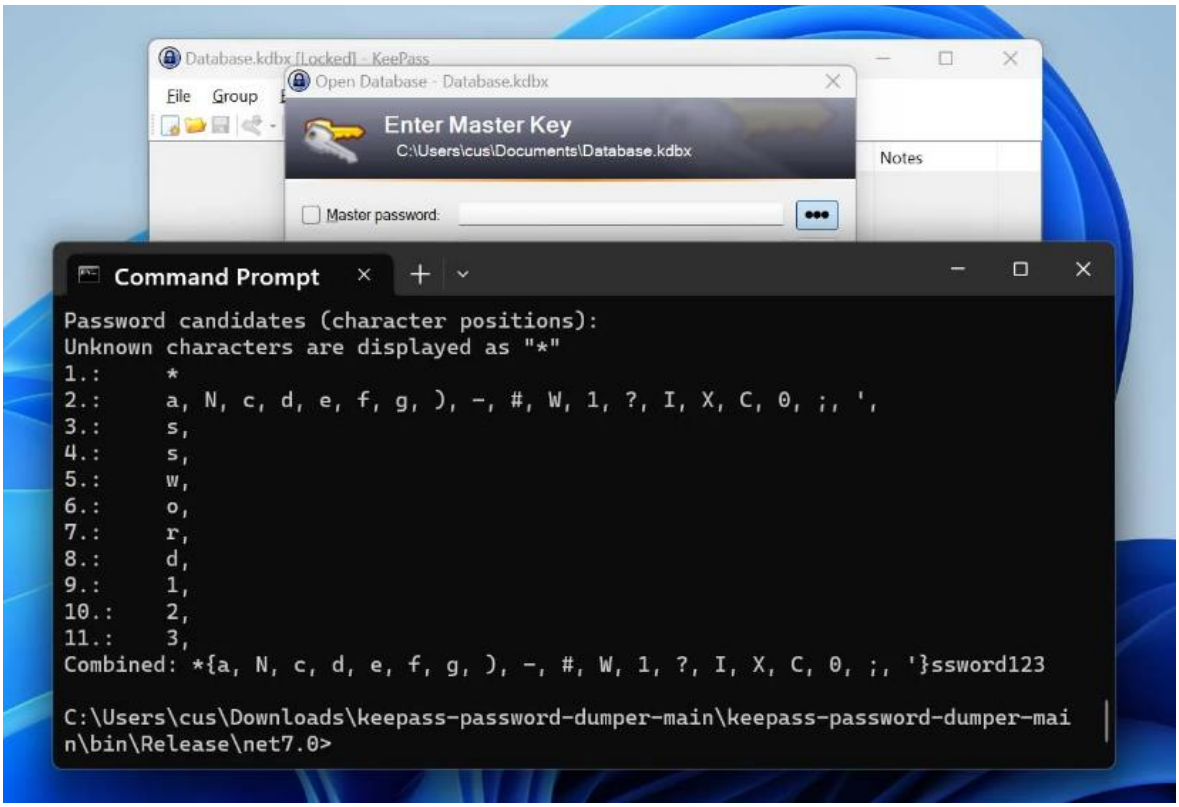


شکل ۱. ایجاد پایگاه داده آزمایشی KeePass

سپس فضای‌کاری KeePass خود را قفل نمود تا از دسترسی به آن جلوگیری شود مگر اینکه رمزعبور اصلی دوباره وارد شود. در این آزمایش‌ها، می‌توان از Process Explorer برای تخلیه حافظه پروژه KeePass استفاده نمود، اما برای درست کار کردن نیاز به تخلیه کامل حافظه است، نه فقط یک تخلیه کوچک.[۱] برای تخلیه حافظه فرآیندها، به هیچ دسترسی بالایی نیاز نیست. BleepingComputer پس از کامپایل کردن ابزار

[۱] minidump

keepass-password-dumper با استفاده از ویژوال استودیو، آن را در برابر تخلیه حافظه خود اجرا نمود و مطابق شکل زیر سریعا بیشتر رمزعبور متن عادی را بازیابی نمود، فقط دو حرف اول از قلم افتاده بود.



شکل ۲. استخراج بیشتر رمز عبور اصلی KeePass

در حالی که این رمزعبور کامل نیست، اما تعیین این‌که چه کاراکترهایی از قلم افتاده‌اند کار بسیار آسانی است. محقق همچنین هشدار می‌دهد که رمزهای عبور اصلی استفاده شده در گذشته می‌توانند در حافظه باقی بمانند و حتی اگر KeePass دیگر روی رایانه مورد نفوذ اجرا نشود باز هم می‌توان آن‌ها را بازیابی کرد.

۴ اصلاح، به زودی...

دومینیک ریچل توسعه‌دهنده KeePass، گزارش باگ را دریافت کرد و قول داد که در نسخه 2.54 یک اصلاح برای CVE-2023-32784 ارائه نماید که انتظار می‌رود در جولای ۲۰۲۳ باشد. با این حال، ریچل به BleepingComputer گفت که نسخه KeePass 2.54 به احتمال زیاد حدود دو هفته دیگر برای کاربران عرضه خواهد شد. بر اساس بحثی که ریچل دیدگاه خود را در مورد این نقص امنیتی و استراتژی‌های کاهش بلاقوه آن ارائه داد، دو پیشرفت امنیتی برای نسخه آینده KeePass ذکر شده است:

- فراخوانی‌های مستقیم API برای دریافت/تنظیم متن، از جعبه‌متنی انجام شود، از ایجاد رشته‌های مدیریت‌شده در حافظه که می‌توانند منجر به فاش شدن اطلاعات شوند، اجتناب شود.
- قطعات مصنوعی و ساختگی حاوی کاراکترهای تصادفی در حافظه پردازش ایجاد شود که طول آن ها تقریباً به اندازه رمزعبور اصلی کاربر باشد تا دستیابی به رمز عبور اصلی را مبهم می‌سازد.

KeePass نسخه 2.54 برای ویندوز، هر دو مورد بالا را دارا خواهد بود، در حالی که نسخه‌های macOS و Linux تنها پیشرفت دوم را دریافت خواهند کرد. خالق PoC تایید کرده است که با وجود دو پیشرفت امنیتی ذکر شده در بالا، دیگر نمی‌تواند حمله را تکرار کند، بنابراین به نظر می‌رسد که این اصلاح موثر واقع شود.

حتی پس از انتشار نسخه جدید، رمزعبور اصلی ممکن است همچنان در فایل‌های حافظه ذخیره شود. این محقق هشدار می‌دهد که برای اینکه مطمئن باشید ۱۰۰٪ خطری در کمین سیستم شما نیست، باید فایل‌های swap و hibernation سیستم خود را حذف کنید، هارد دیسک خود را با استفاده از حالت "overwrite data" فرمت کنید و سیستم عامل را مجددا نصب کنید تا از بازیابی اطلاعات جلوگیری شود.

با این حال، برای بسیاری از افراد، راه‌اندازی مجدد رایانه، پاک کردن فایل‌های swap و hibernation و عدم استفاده از KeePass تا زمان انتشار نسخه جدید، اقدامات ایمنی معقولی به حساب می‌آید. حتی با این وجود برای محافظت بهتر، برنامه‌ها را از سایت‌های نامعتبر دانلود نکنید و مراقب حملات فیشینگ که ممکن است دستگاه‌های شما را آلوده کند و به عوامل تهدید دسترسی از راه دور به دستگاه و پایگاه‌داده KeePass شما را بدهد، باشید.

۵ منابع خبر

[1] https://www.bleepingcomputer.com/news/security/keepass-exploit-helps-retrieve-cleartext-master-password-fix-coming-soon/