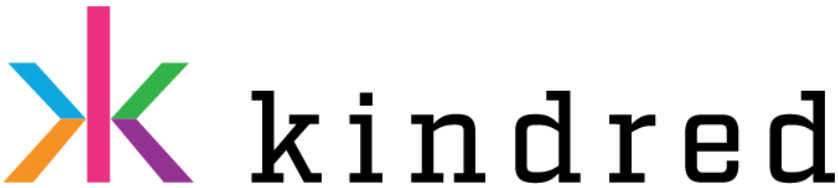

Security Newsletter

22 May 2023

Subscribe to this newsletter

KeePass exploit helps retrieve cleartext master password, fix coming soon

The popular KeePass password manager is vulnerable to extracting the master password from the application's memory, allowing attackers who compromise a device to retrieve the password even with the database is locked.

The issue was discovered by a security researcher known as 'vdohney,' who published a proof-of-concept tool allowing attackers to extract the KeePass master password from memory as a proof-of-concept (PoC). Password managers allow users to create unique passwords for every online account and store the credentials in an easy-to-search database, or password vault, so you do not have to remember each one. However, to properly secure this password vault, users must remember the one master password used to unlock it and access stored credentials.

This master password encrypts the KeePass password database, preventing it from being opened or read without first entering the password. However, once that master password is compromised, a threat actor can access all the credentials stored in the database. Therefore, for a password manager to be properly secured, it is critical that users guard the master password and not share it with anyone else.

Read More

More #News

- PyPI temporarily pauses new users, projects amid high volume of malware
- Apple fixes three new zero-days exploited to hack iPhones, Macs
- 18-year-old charged with hacking 60,000 DraftKings betting accounts
- Dish Network likely paid ransom after recent ransomware attack

#Breach Log

- Android phones are vulnerable to fingerprint brute-force attacks
- The Week in Ransomware - May 19th 2023 - A Shifting Landscape
- Microsoft: Notorious FIN7 hackers return in Clop ransomware attacks

#Patch Time!

- Apple fixes three new zero-days exploited to hack iPhones, Macs
- Microsoft pulls Defender update fixing Windows LSA Protection bug
- Windows 11 KB5026372 cumulative update released with 20 changes

#Tech and #Tools

- Cloned CapCut websites push information stealing malware
- Microsoft shares more info on the end of Internet Explorer
- ASUS routers knocked offline worldwide by bad security update

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us