Overall rating: High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a recently disclosed vulnerability in KeePassXC through 2.7.5.

Technical Details

A local attacker can make changes to the Database security settings, including master password and second-factor authentication, within an authenticated KeePassXC Database session, without the need to authenticate these changes by entering the password and/or second-factor authentication to confirm changes.

This vulnerability is rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-35866
- https://github.com/keepassxreboot/keepassxc/issues/9339
- https://github.com/keepassxreboot/keepassxc/issues/9391