May 28, 2024

Overall Rating - High

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Foxit published security advisories to address vulnerabilities in the following products:

- Foxit PDF Editor for Windows – multiple versions
- Foxit PDF Reader for Windows – versions prior to 2024.2.1.25153
- Foxit PDF Editor for Mac – multiple versions
- Foxit PDF Reader for Mac – versions prior to 2024.2.1.64379

.

Technical Details

Addressed potential issues where the application could be exposed to Time-of-Check Time-of-Use (TOCTOU) Race Condition or Privilege Escalation vulnerability when performing an update, which attackers could exploit to carry out privilege escalation attacks by replacing the update file with a malicious one. This occurs as the application fails to properly validate the certificate of the updater executable or fails to lock the permissions of the update file after certificate validation. (CVE-2024-29072)
These vulnerabilities are rated as an overall **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-2024-29072
- Foxit Security Bulletins