August 27, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

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

- Foxit PDF Editor for Windows – multiple versions
- Foxit PDF Reader for Windows – versions 2024.2.2.25170 and prior
- Foxit PDF Editor for Mac – 2024.2.2.64388, 2024.2.1.64379, 2024.2.0.64371, and 2024.1.0.63682

Technical Details

Addressed potential issues where the application could be exposed to a Use-After-Free vulnerability and crash when handling certain Doc objects or AcroForms, which attackers could exploit to execute remote code or disclose information. This occurs due to the use of a wild pointer or an object that has been freed without proper validation. (CVE-2024-7722, CVE-2024-7723, CVE-2024-7724, CVE-2024-7725)

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- Foxit Security Bulletins