September 12, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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

- Acrobat Reader DC – version 24.003.20054 and prior (Windows), version 24.002.21005 and prior (MacOS)

Adobe Acrobat Reader after a fix was released yesterday for a remote code execution zero-day with a public in-the-wild proof-of-concept exploit.

Technical Details

The flaw is tracked as CVE-2024-41869 and is a critical use after free vulnerability that could lead to remote code execution when opening a specially crafted PDF document.

A "use after free" bug is when a program tries to access data in a memory location that has already been freed or released. This causes unexpected behavior, such as a program crashing or freezing.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

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

- CVE-2024-41869 CVE-2024-45112
- Adobe fixes Acrobat Reader zero-day with public PoC exploit (bleepingcomputer.com)
- Adobe Security Advisories