May 14, 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 Adobe published security advisories to address vulnerabilities in the following products:

- Acrobat DC – version 24.002.20736 and prior
- Acrobat Reader DC – version 24.002.20736 and prior
- Acrobat 2020 – version 20.005.30574 and prior
- Acrobat Reader 2020 – version 20.005.30574 and prior
- Adobe Animate 2023 – version 23.0.5 and prior
- Adobe Animate 2024 – version 24.0.2 and prior
- Adobe Dreamweaver – version 21.3 and prior
- Adobe FrameMaker – versions 2020 Release Update 5 and 2022 Release Update 3 and prior
- Adobe Substance 3D Designer – version 13.1.1 and prior
- Adobe Substance 3D Painter – version 9.1.2 and prior
- Aero – version 0.23.4 and prior
- Illustrator 2023 – version 27.9.3 and prior
- Illustrator 2024 – version 28.4 and prior

Technical Details

Adobe recommends users update their software installations to the latest versions by following the instructions below.
The latest product versions are available to end users via one of the following methods:

- Users can update their product installations manually by choosing Help > Check for Updates.
- The products will update automatically, without requiring user intervention, when updates are detected.
- The full Acrobat Reader installer can be downloaded from the Acrobat Reader Download Center.

For IT administrators (managed environments):

- Refer to the specific release note version for links to installers.
- Install updates via your preferred methodology, such as AIP-GPO, bootstrapper, SCUP/SCCM (Windows), or on macOS, Apple Remote Desktop and SSH.

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-2024-34097 CVE-2024-34098 CVE-2024-34099 CVE-2024-34100 CVE-2024-30311 CVE-2024-30312 CVE-2024-34101 CVE-2024-20791 CVE-2024-20792 CVE-2024-20793 CVE-2024-30274 CVE-2024-30307 CVE-2024-30308 CVE-2024-30309 CVE-2024-30275 CVE-2024-30281 CVE-2024-30282 CVE-2024-30293 CVE-2024-30294 CVE-2024-30295 CVE-2024-30296 CVE-2024-30297 CVE-2024-30298 CVE-2024-30288 CVE-2024-30291 CVE-2024-30289 CVE-2024-30292 CVE-2024-30290 CVE-2024-30287 CVE-2024-30286 CVE-2024-30283
- Adobe Security Advisories