June 12, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Adobe has released their Security Advisory for multiple Adobe Products.

Technical Details

Adobe has released an update for *Photoshop for Windows and macOS*. This update resolves a critical vulnerability. Successful exploitation could lead to arbitrary code execution. CVE-2024-20753, and CVE-2024-26029 are assessed as HIGH risks.

Adobe has released updates for *Adobe Experience Manager (AEM)*. These updates resolve vulnerabilities rated critical, important and moderate. Successful exploitation of these vulnerabilities could result in arbitrary code execution, arbitrary file system read and security feature bypass.

Adobe has released an update for *Adobe Audition for Windows and macOS*. This update resolves important memory leak and application denial-of-service vulnerabilities.

Adobe has released an update for *Adobe Media Encoder*. This update resolves an important vulnerability that could lead to memory leak.

Adobe has released a security update for *Adobe FrameMaker Publishing Server*. This update addresses critical vulnerabilities. Successful exploitation could lead to privilege escalation. ***CVE-2024-30299, and CVE-2024-30300 are assessed as CRITICAL.***

Adobe has released a security update for *Adobe Commerce, Magento Open Source and Adobe Commerce Webhooks Plugin*. This update resolves critical and important vulnerabilities. Successful exploitation could lead to arbitrary code execution, security feature bypass and privilege escalation. ***CVE-2024-34102 and CVE-2024-34108 have been assessed as CRITICAL vulnerabilities.***

Adobe has released security updates for *ColdFusion versions 2023 and 2021*. These updates resolve important vulnerabilities that could lead to arbitrary file system read and security feature bypass.

Adobe has released an update for *Adobe Substance 3D Stager*. This update addresses a critical vulnerability in Adobe Substance 3D Stager. Successful exploitation could lead to arbitrary code execution in the context of the current user.

Adobe has released an update for the *Creative Cloud Desktop for Windows and macOS*. This update includes a fix for a critical vulnerability that could lead to arbitrary code execution in the context of the current user.

Adobe has released a security update for *Adobe Acrobat Android*. This update addresses important vulnerabilities. Successful exploitation could lead to security feature bypass.

This vulnerability is rated as a **CRITICAL** 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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- **APSB24-27** : Security update available for Adobe Photoshop
- **APSB24-28** : Security update available for Adobe Experience Manager
- **APSB24-32** : Security update available for Adobe Audition
- **APSB24-34** : Security update available for Adobe Media Encoder
- **APSB24-38** : Security update available for Adobe FrameMaker Publishing Server
- **APSB24-40** : Security update available for Adobe Commerce
- **APSB24-41** : Security update available for Adobe ColdFusion
- **APSB24-43** : Security update available for Adobe Substance 3D Stager
- **APSB24-44** : Security update available for Adobe Creative Cloud Desktop
- **APSB24-50** : Security update available for Adobe Acrobat Android
- Adobe Product Security
- VRM Vulnerability Reports