

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Adobe product security advisories.

Technical Details

- Adobe has released a security update for Adobe Acrobat and Reader for Windows and macOS. This update addresses critical, important and moderate vulnerabilities. Successful exploitation could lead to arbitrary code execution and memory leak. This vulnerability impacts Acrobat DC and Acrobat Reader DC continuous track 23.006.20360 and earlier versions for Windows and macOS platforms; and Acrobat 2020 and Acrobat Reader 2020 classic 2020 track 20.005.30524 and earlier versions for Windows and macOS platforms.
- Adobe has released an update for Photoshop for Windows and macOS. This update resolves critical and important vulnerabilities. Successful exploitation could lead to arbitrary code execution and memory leak. These vulnerabilities impact Photoshop 2023 24.7.1 and earlier versions and Photoshop 2024 25.0 and earlier versions for Windows and macOS platforms.
- Adobe has released security updates for ColdFusion 2023 Update 5 and earlier versions and 2021 Update 11 and earlier versions for all platforms. These updates resolve critical, important and moderate vulnerabilities that could lead to arbitrary code execution and security feature bypass.
- Adobe has released a security update for RoboHelp Server affects RHS 11.4 and earlier versions for Windows platforms. This update resolves vulnerabilities rated critical and important. Successful exploitation could lead to arbitrary code execution and memory leak in the context of the current user.
- Adobe has released a security update for Adobe InDesign. This update addresses important and moderate vulnerabilities. Successful exploitation could lead to application denial-of-service and memory leak. This vulnerability impacts Adobe InDesign ID18.5 and earlier version and ID17.4.2 and earlier version for Windows and macOS platforms.
- Adobe has released a security update for Adobe Bridge. This update addresses moderate vulnerabilities that could lead to memory leak. These vulnerabilities impact Adobe Bridge 13.0.4 and earlier versions and 14.0.0 and earlier versions for Windows and macOS platforms.
- Adobe has released a security update for Adobe FrameMaker Publishing Server. This update addresses a critical vulnerability. Successful exploitation could lead to security feature bypass. The critical vulnerability impacts Adobe FrameMaker Publishing Server 2022 and earlier versions for Windows platforms.
- Adobe has released a security update for Adobe InCopy. This update addresses a critical vulnerability. Successful exploitation could lead to arbitrary code execution. Adobe InCopy 18.5 and earlier versions and 17.4.2 and earlier versions for Windows and macOS platforms are affected by these vulnerabilities.
- Adobe has released an update for Adobe Animate. This update resolves an important vulnerability. Successful exploitation could lead to memory leak in the context of the current

user. Adobe Animate 2023 23.0.2 and earlier versions for Windows and macOS are impacted.

- Adobe has released an update for Adobe Dimension. This update addresses an important vulnerability in Adobe Dimension. Successful exploitation could lead to memory leak in the context of the current user. This update resolves vulnerabilities in Adobe Dimension 3.4.9 and earlier versions for Windows and macOS.
- Adobe has released an update for Adobe Media Encoder. This update resolves critical and moderate vulnerabilities that could lead to arbitrary code execution and memory leak. Adobe Media Encoder 24.0.2 and earlier versions and 23.6 and earlier versions for Windows and macOS are impacted.
- Adobe has released an update for Adobe Audition for Windows and macOS. This update resolves critical, important and moderate arbitrary code execution and memory leak vulnerabilities. Versions impacted are Adobe Audition 24.0 and earlier versions and 23.6.1 and earlier versions.
- Adobe has released updates for Adobe Premiere Pro for Windows and macOS. This update addresses critical and moderate vulnerabilities. Successful exploitation could lead to arbitrary code execution and memory leak. Adobe Premiere Pro 24.0 and earlier versions and 23.6 and earlier versions for Windows and macOS platforms are affected.
- Adobe has released an update for Adobe After Effects for Windows and macOS. This update addresses critical and moderate security vulnerabilities. Successful exploitation could lead to arbitrary code execution and memory leak in the context of the current user. These vulnerabilities will affect Adobe After Effects 24.0.2 and earlier versions and 23.6 and earlier versions for Windows and macOS platforms.

These vulnerabilities are rated as high as **CRITICAL** risks. Software updates exist to address these risks. **Please refer to the specified links below for each product for further details.**

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.

References

- CVE-2023-22272, CVE-2023-22273, CVE-2023-22274, CVE-2023-22275, CVE-2023-22268, CVE-2023-44325, CVE-2023-44326, CVE-2023-26347, CVE-2023-26368, CVE-2023-44330, CVE-2023-44331, CVE-2023-44332, CVE-2023-44333, CVE-2023-44334, CVE-2023-44335, CVE-2023-44336, CVE-2023-44337, CVE-2023-44338, CVE-2023-44339, CVE-2023-44340, CVE-2023-44341, CVE-2023-44342, CVE-2023-44343, CVE-2023-44344, CVE-2023-44345, CVE-2023-44346, CVE-2023-44347, CVE-2023-44348, CVE-2023-44350, CVE-2023-44351, CVE-2023-44352, CVE-2023-44353, CVE-2023-44355, CVE-2023-44356, CVE-2023-44357, CVE-2023-44358, CVE-2023-44359, CVE-2023-44360, CVE-2023-44361, CVE-2023-44365, CVE-2023-44366, CVE-2023-44367, CVE-2023-44371, CVE-2023-44372, CVE-2023-47040, CVE-2023-47041, CVE-2023-47042, CVE-2023-47043, CVE-2023-47044, CVE-2023-47055, CVE-2023-47056, CVE-2023-47057, CVE-2023-47058, CVE-2023-47059, CVE-2023-47060
- [Security updates available for Adobe ColdFusion | APSB23-52](#)
- [Security hotfix available for RoboHelp Server | APSB23-53](#)
- [Security update available for Adobe Acrobat and Reader | APSB23-54](#)
- [Security Update Available for Adobe InDesign | APSB23-55](#)
- [Security update available for Adobe Photoshop | APSB23-56](#)
- [Security Updates Available for Adobe Bridge | APSB23-57](#)
- [Security Updates Available for Adobe FrameMaker Publishing Server | APSB23-58](#)
- [Security Update Available for Adobe InCopy | APSB23-60](#)
- [Security updates available for Adobe Animate | APSB23-61](#)
- [Security updates available for Dimension | APSB23-62](#)
- [Security Updates Available for Adobe Media Encoder | APSB23-63](#)

- [Security Updates Available for Adobe Audition | APSB23-64](#)
- [Security Updates Available for Adobe Premiere Pro | APSB23-65](#)
- [Security Updates Available for Adobe After Effects | APSB23-66](#)
- [Adobe Security Bulletins and Advisories](#)
- [VRM Vulnerability Reports](#)