



Adobe Security Bulletin

Last updated on Apr 12, 2026

Security update available for Adobe Acrobat Reader | APSB26-43

Bulletin ID	Date Published	Priority
APSB26-43	April 11, 2026	1

Summary

Adobe has released a security update for Adobe Acrobat and Reader for Windows and macOS. This update addresses a [critical](#) vulnerability. Successful exploitation could lead to arbitrary code execution.

Adobe is aware of CVE-2026-34621 being exploited in the wild.

Affected Versions

Product	Track	Affected Versions	Platform
Acrobat DC	Continuous	26.001.21367 and earlier	Windows & macOS
Acrobat Reader DC	Continuous	26.001.21367 and earlier	Windows & macOS
Acrobat 2024	Classic 2024	24.001.30356 and earlier	Windows & macOS

For questions regarding Acrobat DC, please visit the [Acrobat DC FAQ page](#).

For questions regarding Acrobat Reader DC, please visit the [Acrobat Reader DC FAQ page](#).

Solution

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.

Adobe categorizes these updates with the following [priority ratings](#) and recommends users update their installation to the newest version:

Product	Track	Updated Versions	Platform	Priority Rating	Availability
Acrobat DC	Continuous	26.001.21411	Windows and macOS	1	Release Notes
Acrobat Reader DC	Continuous	26.001.21411	Windows and macOS	1	Release Notes
Acrobat 2024	Classic 2024	Windows: 24.001.30362 Mac: 24.001.30360	Windows and macOS	1	Release Notes

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVSS base score	CVSS vector
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (CWE-1321)	Arbitrary code execution	Critical	8.6	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Acknowledgements


Adobe would like to thank the following researchers for reporting these issues and for working with Adobe to help protect our customers:

- Haifei Li (EXPMON) - CVE-2026-34621

Revisions:

- April 12, 2026: Adjusted CVSS Attack Vector from Network (AV:N) to Local (AV:L), changing the overall CVSS from 9.6 to 8.6.

NOTE: Adobe has a public bug bounty program with HackerOne. If you are interested in working with



[m/adobe](#)
RT@adobe.com.

Get help faster and easier

[Sign in](#)

New user?

[Create an account >](#)



Share this page



Was this page helpful?

Yes, thanks

Not really



Ask the
Community

Post questions and get
answers from experts.

[Ask now](#)



Contact Us

Expert support for your
issues.

[Start now](#)

[^ Back to top](#)