

Adobe Security Bulletin

Last updated on Apr 14, 2026

Security update available for Adobe Connect | APSB26-37

Bulletin ID	Date Published	Priority
APSB26-37	April 14, 2026	3

Summary

Adobe has released a security update for Adobe Connect. This update resolves [critical](#) and [important](#) vulnerabilities that could lead to arbitrary code execution and privilege escalation.

Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.

Affected Product Versions

Product	Version	Platform
Adobe Connect	12.10 and earlier	Windows and macOS
Adobe Connect Desktop Application	2025.3 and earlier	Windows and macOS

Solution

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

Product	Version	Platform	Priority	Availability
Adobe Connect	12.11	Windows and macOS	3	Release Notes
Adobe Connect Desktop Application	2025.9	Windows	3	Release Notes

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVSS base score	CVSS vector
Deserialization of Untrusted Data (CWE-502)	Arbitrary code execution	Critical	9.6	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:+
Deserialization of Untrusted Data (CWE-502)	Arbitrary code execution	Critical	9.6	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:+
Cross-site Scripting (Reflected XSS) (CWE-79)	Arbitrary code execution	Critical	9.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:+

Cross-site Scripting (Reflected XSS) (CWE-79)	Arbitrary code execution	Critical	9.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
Cross-site Scripting (DOM-based XSS) (CWE-79)	Arbitrary code execution	Critical	9.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
Deserialization of Untrusted Data (CWE-502)	Arbitrary code execution	Critical	9.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
Cross-site Scripting (XSS) (CWE-79)	Privilege escalation	Critical	9.6	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
Cross-site Scripting	Arbitrary code	Important		

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

- Laish (a_l) -- CVE-2026-27302, CVE-2026-27303, CVE-2026-34615
- yjdfy -- CVE-2026-21331, CVE-2026-34614
- green-jam -- CVE-2026-27243, CVE-2026-27245, CVE-2026-27246
- remot3 -- CVE-2026-34617

Adobe

Get help faster and easier

Sign in

New user?

[Create an account >](#)


working with


om.

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](#)