Adobe Security Bulletin

Last updated on Apr 28, 2026

Security update available for Adobe Connect | APSB25-70

Bulletin ID	Date Published	Priority
APSB25-70	October 14, 2025	3

Summary

Adobe has released a security update for Adobe Connect. This update resolves critical and moderate vulnerabilities that could lead to arbitrary code execution and security feature bypass.

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	12.9 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	12.10	Windows and macOS	3	Release Notes

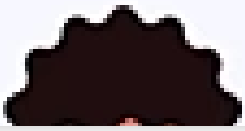
Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVSS base score	CVSS vector
Cross-site Scripting (DOM-based XSS) (CWE-79)	Arbitrary code execution	Critical	8.1	CVSS:3.1/AV:N/AC:L/PR:H/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
URL Redirection to Untrusted Site ('Open Redirect') (CWE-601)	Security feature bypass	Important	4.7	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

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

- Laish (a_l) -- CVE-2025-49552, CVE-2025-49553, CVE-2025-54196

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



om.