Adobe Security Bulletin

Last updated on Apr 14, 2026

Security updates available for Adobe ColdFusion | APSB26-38

Bulletin ID	Date Published	Priority
APSB26-38	April 14, 2026	1

Summary

Adobe has released security updates for ColdFusion versions 2025 and 2023. These updates resolves critical and moderate vulnerabilities that could lead to arbitrary code execution, application denial-of-service, arbitrary file system read, and security feature bypass.

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

Affected Versions

Product	Update number	Platform
ColdFusion 2025	Update 6 and earlier versions	All
ColdFusion 2023	Update 18 and earlier versions	All

Solution

Adobe categorizes these updates with the following priority rating and recommends users update their installations to the newest versions:

Product	Updated Version	Platform	Priority rating	Availability
ColdFusion 2025	Update 7	All	1	Tech Note
ColdFusion 2023	Update 19	All	1	Tech Note

Note

For security reasons, we strongly recommend to use latest mysql java connector. For more information on its usage, please refer to: https://helpx.adobe.com/coldfusion/kb/coldfusion-configuring-mysql-jdbc.html

See the updated serial filter documentation for more details on protection against insecure deserialization attacks: https://helpx.adobe.com/coldfusion/kb/coldfusion-serialfilter-file.html

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	CVSS base score	CVSS vector

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22)	Security feature bypass	Critical	7.7	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H
Improper Input Validation (CWE-20)	Arbitrary code execution	Critical	9.3	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22)	Arbitrary file system read	Critical	8.6	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Improper Input Validation (CWE-20)	Security feature bypass	Critical	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Acknowledgements:

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

- AnirudhAnand (a0xnirudh) -- CVE-2026-27304
- nbxiglk -- CVE-2026-27306
- Jonathan Lein of TrendAI Research -- CVE-2026-27282, CVE-2026-34619, CVE-2026-27305
- Idris_Tester092004 (tester092004) -- CVE-2026-27307, CVE-2026-27308

NOTE: Adobe has a public bug bounty program with HackerOne. If you are interested in working with Adobe as an external security researcher, please check out https://hackerone.com/adobe

Note

Adobe recommends updating your ColdFusion JDK/JRE LTS version to the latest update release as a secure practice. The ColdFusion downloads page is regularly updated to include the latest Java installers for the JDK version your installation supports as per the matrices below.

- *ColdFusion 2025 support matrix*
- *ColdFusion 2023 support matrix*

For instructions on how to use an external JDK, view Change ColdFusion JVM.

Adobe also recommends applying the security configuration settings included in the ColdFusion Security documentation as well as review the respective Lockdown guides.

- *ColdFusion 2025 Lockdown Guide*
- *ColdFusion 2023 Lockdown Guide*

Share this page