



Adobe Security Bulletin

Last updated on Feb 9, 2026

Security updates available for Adobe ColdFusion | APSB25-105

Bulletin ID	Date Published	Priority
APSB25-105	December 9, 2025	1

Summary

Adobe has released security updates for ColdFusion versions 2025, 2023 and 2021. These updates resolves [critical](#) and [important](#) vulnerability that could lead to arbitrary file system write, arbitrary file system read, arbitrary code execution, security feature bypass, and privilege escalation.

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 4 and earlier versions	All
ColdFusion 2023	Update 16 and earlier versions	All
ColdFusion 2021	Update 22 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 5	All	1	Tech Note
ColdFusion 2023	Update 17	All	1	Tech Note
ColdFusion 2021	Update 23	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
------------------------	----------------------	----------	-----------------	-----------------------------

Unrestricted Upload of File with Dangerous Type (CWE-434)	Arbitrary code execution	Critical	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:F
Improper Input Validation (CWE-20)	Security feature bypass	Critical	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:F
Deserialization of Untrusted Data (CWE-502)	Arbitrary code execution	Critical	8.4	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:F
Deserialization of Untrusted Data (CWE-502)	Arbitrary code execution	Critical	8.2	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:F
Improper Access Control (CWE-284)	Arbitrary code execution	Critical	8.4	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:F
Improper Input Validation (CWE-20)	Arbitrary code execution	Critical	8.4	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:F

Acknowledgements:

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

- Brian Reilly (reillyb) -- CVE-2025-61809
- Brian Reilly (reillyb); Vladislav Berghici of TrendAI Research -- CVE-2025-61808

- Nhien Pham (nhienit2010) -- CVE-2025-61812, CVE-2025-61822, CVE-2025-61823
- nbxiglk -- CVE-2025-61810, CVE-2025-61811, CVE-2025-61813, CVE-2025-61821, CVE-2025-61830
- Karol Mazurek (cr1m5on) -- CVE-2025-64897
- bytehacker_sg -- CVE-2025-64898

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](#)
- [ColdFusion 2021 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](#)
- [ColdFusion 2021 Lockdown Guide](#)

Adobe

Get help faster and easier

Sign in

New user?


[Create an account >](#)


[Legal Notices](#) | [Online Privacy Policy](#)

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](#)