Adobe Security Bulletin

Last updated on Oct 16, 2025

Security update available for Adobe Commerce | APSB25-94

Bulletin ID	Date Published	Priority
APSB25-94	October 14, 2025	2

Summary

Adobe has released a security update for Adobe Commerce and Magento Open Source. This update resolves critical and important vulnerabilities. Successful exploitation could lead to security feature bypass, privilege escalation, and arbitrary code execution.

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

Affected Versions

Product	Version	Priority Rating	Platform
Adobe Commerce	2.4.9-alpha2 and earlier 2.4.8-p2 and earlier 2.4.7-p7 and earlier 2.4.6-p12 and earlier 2.4.5-p14 and earlier 2.4.4-p15 and earlier	2	All

Adobe Commerce B2B	1.5.3-alpha2 and earlier 1.5.2-p2 and earlier 1.4.2-p7 and earlier 1.3.5-p12 and earlier 1.3.4-p14 and earlier 1.3.3-p15 and earlier	2	All
Magento Open Source	2.4.9-alpha2 2.4.8-p2 and earlier 2.4.7-p7 and earlier 2.4.6-p12 and earlier	2	All

Solution

Adobe categorizes these updates with the following priority ratings and recommends users update their installation to the newest version.

Product	Updated Version	Platform	Priority Rating	Installation Instructions
Adobe Commerce	2.4.9-alpha3 for 2.4.9-alpha2 2.4.8-p3 for 2.4.8-p2 and earlier 2.4.7-p8 for 2.4.7-p7 and earlier 2.4.6-p13 for 2.4.6-p12 and earlier 2.4.5-p15 for 2.4.5-p14 and earlier 2.4.4 p16 for 2.4.4-p15 and earlier	All	2	2.4.x release notes
Adobe Commerce B2B	1.5.3-alpha3 for 1.5.3-alpha2 1.5.2-p3 for 1.5.2-p2 and earlier 1.4.2-p8 for 1.4.2-p7 and earlier	All	2	

	1.3.4-p15 for 1.3.4-p14 and earlier 1.3.3-p14 for 1.3.3-p13 and earlier 1.3.3-p16 for 1.3.3-p15 and earlier			
Magento Open Source	2.4.9-alpha3 for 2.4.9-alpha2 2.4.8-p3 for 2.4.8-p2 and earlier 2.4.7-p8 for 2.4.7-p7 and earlier 2.4.6-p13 for 2.4.6-p12 and earlier	All	2	

Adobe categorizes these updates with the following priority ratings and recommends users update their installation to the newest version.

Vulnerability Details

Vulnerability Category	Vulnerability Impact	Severity	Authentication required to exploit?	Exploit requires admin privileges?	CVSS base score	
Incorrect Authorization (CWE-863)	Security feature bypass	Critical	Yes	Yes	8.1	CVSS:3
Cross-site Scripting (Stored XSS) (CWE-79)	Privilege escalation	Critical	Yes	Yes	8.1	CVSS:3
Incorrect Authorization (CWE-863)	Security feature bypass	Important	No	No	5.9	CVSS:3

Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Important	Yes	Yes	4.8	CVSS:3
Incorrect Authorization (CWE-863)	Privilege escalation	Important	Yes	Yes	6.5	CVSS:3

Note

Authentication required to exploit: The vulnerability is (or is not) exploitable without credentials.

Exploit requires admin privileges: The vulnerability is (or is not) only exploitable by an attacker with administrative privileges.

Acknowledgements

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

- Akash Hamal (akashhamal0x01) -- CVE-2025-54263, CVE-2025-54265, CVE-2025-54267
- wohli -- CVE-2025-54264
- Oleksii Suchalkin (schemonah) -- CVE-2025-54266

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.

Revisions

October 15, 2025 -- CVE-2025-54263: Corrected vulernability category, CVSS vector, and CVSS base score.

October 16, 2025 -- Corrected solution version 1.3.4-p15 for 1.3.4-p14 and earlier for Adobe Commerce

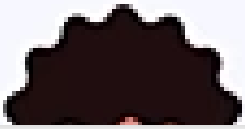
Adobe

Get help faster and easier

Sign in

New user?

Create an account ›



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