Adobe Security Bulletin

Search Adobe Support

Last updated on Apr 8, 2025

Security update available for Adobe Commerce | APSB25-26

Bulletin ID	Date Published	Priority
APSB25-26	April 8, 2025	2

Summary

Adobe has released a security update for Adobe Commerce and Magento Open Source. This update resolves important and moderate vulnerabilities. Successful exploitation could lead to security feature bypass, privilege escalation and application denial-of-service.

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

Affected Versions

Product	Version	Platform
Adobe Commerce	2.4.8-beta2 2.4.7-p4 and earlier 2.4.6-p9 and earlier 2.4.5-p11 and earlier 2.4.4-p12 and earlier	All
Adobe Commerce B2B	1.5.1 and earlier 1.4.2-p4 and earlier 1.3.5-p9 and earlier	All

	1.3.4-p11 and earlier 1.3.3-p12 and earlier	
Magento Open Source	2.4.8-beta2 2.4.7-p4 and earlier 2.4.6-p9 and earlier 2.4.5-p11 and earlier 2.4.4-p12 and earlier	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	2.4.8 for 2.4.8-beta2 2.4.7-p5 for 2.4.7-p4 and earlier 2.4.6-p10 for 2.4.6-p9 and earlier 2.4.5-p12 for 2.4.5-p11 and earlier 2.4.4-p13 for 2.4.4-p12 and earlier	All	2	2.4.x release notes
Adobe Commerce B2B	1.5.2 for 1.5.1 1.4.2-p5 for 1.4.2-p4 and earlier 1.3.5-p10 for 1.3.5-p9 and earlier 1.3.4-p12 for 1.3.4-p11 and earlier 1.3.3-p13 for 1.3.3-p12 and earlier	All	2	
Magento Open Source	2.4.8 for 2.4.8-beta2 2.4.7-p5 for 2.4.7-p4 and earlier 2.4.6-p10 for 2.4.6-p9 and earlier	All	2	

	2.4.5-p12 for 2.4.5-p11 and earlier 2.4.4-p13 for 2.4.4-p12 and earlier			

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	
Improper Authorization (CWE-285)	Privilege escalation	Important	Yes	Yes	4.3	CVSS:3.1/AV:N
Cross-Site Request Forgery (CSRF) (CWE-352)	Application denial-of-service	Important	Yes	Yes	4.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	Yes	Yes	5.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	Yes	Yes	5.3	CVSS:3.1/AV:N
Insufficiently Protected Credentials (CWE-522)	Security feature bypass	Moderate	Yes	Yes	2.7	CVSS:3.1/AV:N

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:

- sheikhrishad0 - CVE-2025-27190, CVE-2025-27191
- Akash Hamal (akashhamal0x01) - CVE-2025-27188
- Bobby Tabl35 (bobbytabl35_) - CVE-2025-27189

erested in working

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

Shop for

For business

For education

For nonprofits

For mobile

Experience Cloud

Support

Resources

Adobe Account

Adobe

Featured products Adobe Acrobat Reader Adobe Express Photoshop Illustrator

Change region

□ Adobe on

□ Adobe on

□ Adobe on

□ Adobe on