Adobe Security Bulletin

Last updated on Feb 11, 2025

Security update available for Adobe Commerce | APSB25-08

Bulletin ID	Date Published	Priority
APSB25-08	February 11, 2025	1

Summary

Adobe has released a security update for Adobe Commerce and Magento Open Source. This update resolves critical, important and moderate vulnerabilities. Successful exploitation could lead to 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	Version	Platform
Adobe Commerce	2.4.8-beta1 2.4.7-p3 and earlier 2.4.6-p8 and earlier 2.4.5-p10 and earlier 2.4.4-p11 and earlier	All
Adobe Commerce B2B	1.5.0 and earlier 1.4.2-p3 and earlier 1.3.5-p8 and earlier	All

	1.3.4-p10 and earlier 1.3.3-p11 and earlier	
Magento Open Source	2.4.8-beta1 2.4.7-p3 and earlier 2.4.6-p8 and earlier 2.4.5-p10 and earlier 2.4.4-p11 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-beta2 for 2.4.8-beta1 2.4.7-p4 for 2.4.7-p3 and earlier 2.4.6-p9 for 2.4.6-p8 and earlier 2.4.5-p11 for 2.4.5-p10 and earlier 2.4.4-p12 for 2.4.4-p11 and earlier	All	2	2.4.x release notes
Adobe Commerce B2B	1.5.1 and earlier 1.4.2-p4 for 1.4.2-p3 and earlier 1.3.5-p9 for 1.3.5-p8 and earlier 1.3.4-p11 for 1.3.4-p10 and earlier 1.3.3-p12 for 1.3.3-p11 and earlier	All	2	
Magento Open Source	2.4.8-beta2 for 2.4.8-beta1 2.4.7-p4 for 2.4.7-p3 and earlier	All	2	

	2.4.6-p9 for 2.4.6-p8 and earlier 2.4.5-p11 for 2.4.5-p10 and earlier 2.4.4-p12 for 2.4.4-p11 and earlier			
Adobe Commerce and Magento Open Source	Isolated patch for CVE-2025-24434	All	1	Release Notes for Isolated Patch on CVE-2025-24434

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22)	Privilege escalation	Critical	Yes	Yes	7.5	CVSS:3.1/AV:N
Incorrect Authorization (CWE-863)	Security feature bypass	Critical	Yes	No	7.1	CVSS:3.1/AV:N
Information Exposure (CWE-200)	Privilege escalation	Critical	Yes	Yes	8.1	CVSS:3.1/AV:N
Improper Authorization	Security feature bypass	Critical	Yes	No	8.2	CVSS:3.1/AV:N

(CWE-285)						
Improper Authorization (CWE-285)	Privilege escalation	Critical	No	No	9.4	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.7	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Critical	Yes	Yes	8.8	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.7	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N

Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Critical	Yes	Yes	8.9	CVSS:3.1/AV:N
Violation of Secure Design Principles (CWE-657)	Privilege escalation	Important	Yes	No	6.5	CVSS:3.1/AV:N
Incorrect Authorization (CWE-863)	Security feature bypass	Important	Yes	No	4.3	CVSS:3.1/AV:N
Incorrect Authorization (CWE-863)	Security feature bypass	Important	Yes	No	4.3	CVSS:3.1/AV:N
Incorrect Authorization (CWE-863)	Security feature bypass	Important	Yes	Yes	4.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	No	No	6.5	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Privilege escalation	Important	Yes	No	4.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Privilege escalation	Important	Yes	Yes	4.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Privilege escalation	Important	Yes	Yes	4.3	CVSS:3.1/AV:N

Improper Access Control (CWE-284)	Privilege escalation	Important	Yes	Yes	5.4	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	Yes	No	6.5	CVSS:3.1/AV:N
Business Logic Errors (CWE-840)	Security feature bypass	Important	Yes	No	5.3	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	Yes	No	6.5	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Important	Yes	Yes	6.5	CVSS:3.1/AV:N
Cross-site Scripting (Stored XSS) (CWE-79)	Arbitrary code execution	Important	Yes	No	5.4	CVSS:3.1/AV:N
Improper Access Control (CWE-284)	Security feature bypass	Moderate	Yes	Yes	3.5	CVSS:3.1/AV:N
Time-of-check Time-of-use (TOCTOU) Race Condition (CWE-367)	Security feature bypass	Moderate	No	No	3.7	CVSS:3.1/AV:N
Time-of-check Time-of-use	Security feature bypass	Moderate	No	No	3.7	CVSS:3.1/AV:N

(TOCTOU) Race Condition (CWE-367)						

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-2025-24411, CVE-2025-24418, CVE-2025-24419, CVE-2025-24420, CVE-2025-24421, CVE-2025-24422, CVE-2025-24423, CVE-2025-24424, CVE-2025-24425, CVE-2025-24426, CVE-2025-24427, CVE-2025-24429, CVE-2025-24435, CVE-2025-24437
- wohlie - CVE-2025-24408, CVE-2025-24410, CVE-2025-24412, CVE-2025-24413, CVE-2025-24414, CVE-2025-24415, CVE-2025-24416, CVE-2025-24417, CVE-2025-24436, CVE-2025-24438
- thlassche - CVE-2025-24409, CVE-2025-24428, CVE-2025-24434
- Alexandrio - CVE-2025-24407
- g0ndaar - CVE-2025-24430
- sheikhrishad0 - CVE-2025-24432

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

Real help from real people.

Start now

^ Back to top

Featured products Adobe Acrobat Reader Adobe Express Photoshop Illustrator

Change region

Adobe on Facebook
Adobe on Twitter
Adobe on LinkedIn
Adobe on Instagram