CYBER ADVISORY

Friday, October 24, 2025 **CAL-CSIC-202510-A-008**

Critical Remote Code Execution in Adobe Commerce and Magento Open Source

Improper Input Validation	RCE	Arbitrary Code Execution	Full System Compromise

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability known as CVE-2025-54236, with a CVSS v3.1 score of 9.8.[1] This vulnerability is due to improper input validation and would allow a remote, unauthenticated attacker to execute arbitrary code on the affected server. Successful exploitation could lead to full system compromise and unauthorized access to customer and financial data. Adobe is aware of CVE-2025-54236 being exploited in the wild.

The Cal-CSIC recommends immediately updating the latest versions of Adobe Commerce, B2B, and Magento Open Source using the vendor-provided security patch.

For further information on applying remediation steps, please refer to the link provided below.[2]

Adobe Security Bulletin

Affected Products and Versions

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

Adobe Commerce B2B:

- 1.5.3-alpha2 and earlier
- 1.5.2-p2 and earlier
- 1.4.2-p7 and earlier
- 1.3.4-p14 and earlier
- 1.3.3-p15 and earlier

Magento Open Source:

- 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

References

[1]Adobe; "Security Bulletin for Adobe Commerce and Magento Open Source;" https://helpx.adobe.com/security/products/magento/apsb25-88.html; accessed 24 October 2025

[2] CVE; "CVE-2025-54236;" https://www.cve.org/CVERecord?id=CVE-2025-54236"; accessed 24 October 2025