



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

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

¹Adobe; "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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR