National Cyber Security Centre

2407180186-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Adobe Commerce (CVE-2024-34102, CVSSv3: 9.8)

Thursday 18th July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-06-13T09:15:00
Vendor: Adobe
Product: Adobe Commerce
CVE ID: CVE-2024-34102
CVSS3.0 Score[1]**:** 9.8
EPSS[2]**:** 0.997960000
Summary: Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.

More information related to this issue can be found at the following links:

- https://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://www.vicarius.io/vsociety/posts/cosmicsting-critical-unauthenticated-xxe-vulnerability-in-adobe-commerce-and-magento-cve-2024-34102

Products Affected

- Adobe Adobe Commerce

Impact

Common Weakness Enumeration (CWE)[3]**:** Improper Restriction of XML External Entity Reference ('XXE') (CWE-611)

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** YES

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Adobe.

Additional recommendations and mitigations for CVE-2024-34102 can be found in the respective links below:

- https://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://www.vicarius.io/vsociety/posts/cosmicsting-critical-unauthenticated-xxe-vulnerability-in-adobe-commerce-and-magento-cve-2024-34102

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre