Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Wild Exploitation of Critical Flaw in Adobe Commerce and Magento

Date of Publication	Admiralty Code	TA Number
July 19, 2024	A1	TA2024278

Summary

First Seen: June 2024
Affected Products: Adobe Commerce and Magento
Impact: A critical unauthenticated XXE (XML External Entity) vulnerability has been discovered in Adobe Commerce and Magento, identified as CVE-2024-34102. This flaw, assigned a CVSS score of 9.8, is due to improper restriction of XML external entity references. The vulnerability allows attackers to execute arbitrary code by sending a crafted XML document that references external entities. Exploiting this issue does not require user interaction, and the vulnerability is actively being exploited in attacks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-34102	CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)	Adobe Commerce and Magento Open Source	✗	✓	✓

Vulnerability Details

#1 Adobe has issued a warning about a serious vulnerability in Adobe Commerce, identified as CVE-2024-34102, which is being actively exploited in attacks. This flaw has a CVSS score of 9.8 and is an improper restriction of XML external entity (XXE) reference, potentially allowing attackers to execute arbitrary code.

#2 Magento and Adobe Commerce are leading e-commerce platforms for creating and managing online stores. Magento, owned by Adobe, offers extensive customization options and robust features for businesses of all sizes. Adobe Commerce, the enterprise version of Magento, integrates seamlessly with Adobe's marketing and analytics tools, making it ideal for large-scale operations.

#3 The security flaw in Adobe Commerce and Magento, CVE-2024-34102, dubbed "CosmicSting," enables XML External Entity (XXE) injection attacks, leading to sensitive data disclosure. Attackers can craft custom JSON payloads that reference remote Document Type Definition (DTD) files, which are deserialized on the server, exfiltrating data to a specified URL.

#4 This vulnerability also permits unauthorized admin access to REST API, GraphQL API, or SOAP API, resulting in data theft, service disruption, and system compromise. The broader implications of XXE vulnerabilities allow attackers to retrieve and manipulate data from external sources. Additionally, this flaw can be combined with other vulnerabilities, such as the recent PHP iconv flaw (CVE-2024-2961), further increasing the risk of remote code execution.

#5 This flaw affects nearly 75% of websites using Adobe Commerce and Magento and is being actively exploited in the wild. Organizations should invest in continuous security assessments to safeguard their systems from evolving threats and continuously improve cybersecurity to stay ahead of potential vulnerabilities. This proactive approach ensures that security measures are regularly updated, reducing the risk of exploitation and enhancing the overall resilience of their IT infrastructure.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-34102	Adobe Commerce: Versions before: 2.4.7; 2.4.6-p5; 2.4.5-p7; 2.4.4-p8; 2.4.3-ext-7 ; 2.4.2-ext-7 Magento Open Source: Versions before: 2.4.7; 2.4.6-p5; 2.4.5-p7; 2.4.4-p8 Adobe Commerce Webhooks Plugin: Versions 1.2.0 to 1.4.0	cpe:2.3:a:adobe:commerce:*:*:*:*:*:*:*:* cpe:2.3:a:adobe:magento:*:*:open_source:*:*:* cpe:2.3:a:adobe:commerce_webhooks:*:*:*:*:*:*:*:*:*	CWE-611

Recommendations

Update: Users are strongly advised to upgrade to the latest versions to mitigate the CVE-2024-34102 vulnerability. The recommended versions are Adobe Commerce and Magento Open Source versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, and 2.4.4-p9, as well as Adobe Commerce Webhooks Plugin version 1.5.0.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts for XML External Entity (XXE) injection, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access
TA0010 Exfiltration	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	T1606 Forge Web Credentials	T1649 Steal or Forge Authentication Certificates	T1567 Exfiltration Over Web Service

Patch Details

Users are strongly advised to upgrade to the latest versions to mitigate the CVE-2024-34102 vulnerability. The recommended versions are Adobe Commerce and Magento Open Source 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, and 2.4.4-p9, as well as Adobe Commerce Webhooks Plugin version 1.5.0.

Links:
https://experienceleague.adobe.com/en/docs/commerce-operations/release/notes/security-patches/2-4-7-patches

https://experienceleague.adobe.com/en/docs/commerce-operations/upgrade-guide/modules/upgrade

References

https://www.vicarius.io/vsociety/posts/cosmicsting-critical-unauthenticated-xxe-vulnerability-in-adobe-commerce-and-magento-cve-2024-34102

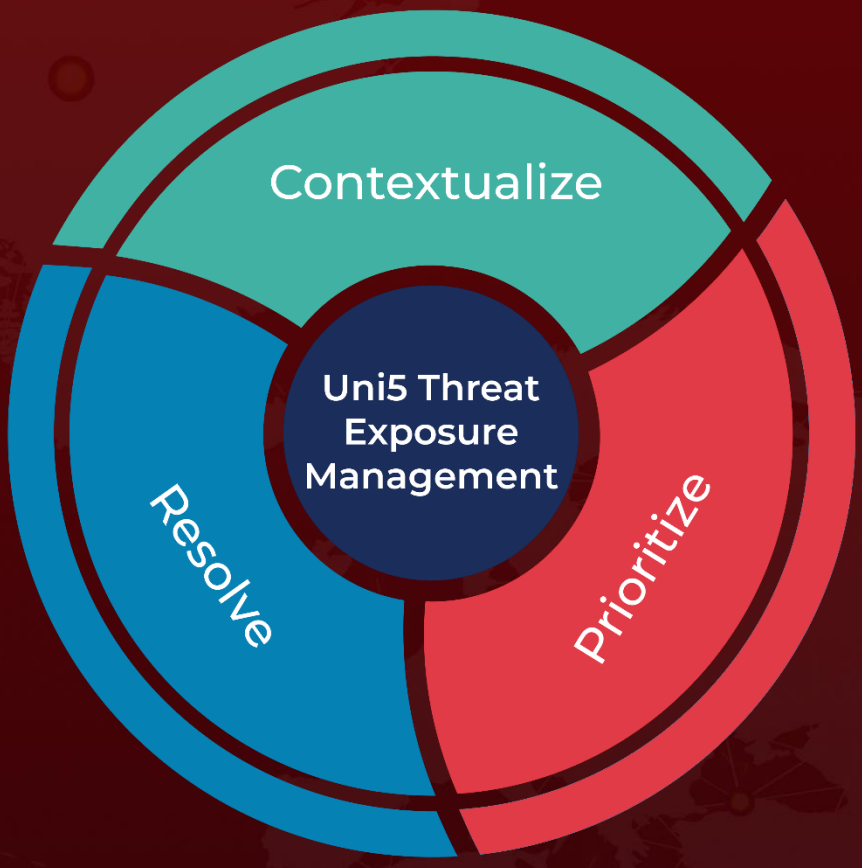
https://helpx.adobe.com/security/products/magento/apsb24-40.html

https://x.com/sansecio/status/1803010319066755234

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 19, 2024 • 7:30 AM

More at www.hivepro.com