BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

June 25, 2024

Adobe Commerce and Magento Sites exposed to CosmicSting Vulnerability

Summary

A recently discovered "CosmicSting" vulnerability affecting Adobe Commerce and Magento websites remains unpatched across the majority of deployed sites, risking catastrophic attacks. Sansec reports that three-quarters of affected websites have not applied the patch, leaving them vulnerable to XML external entity injection (XXE) and remote code execution (RCE).

CVE-ID	CVSSv3 Score
CVE-2024-34102	9.8

Threat intelligence

- No reported exploits in the wild.
- Highly exploitable.

Vulnerability Details

The CosmicSting vulnerability (CVE-2024-34102) is a critical flaw that affects Adobe Commerce and Magento platforms, allowing attackers to read sensitive files and potentially execute remote code. This vulnerability is considered the most severe flaw in these platforms over the past two years.

The primary risk stems from XML external entity injection (XXE) and can escalate to remote code execution (RCE) when combined with the iconv bug in Linux.

Sansec statistics show that about 75% of websites using the affected platforms have not applied the patch for CosmicSting, leaving them vulnerable. Attack methods are easily inferred from the patch code, making the vulnerability highly exploitable. CosmicSting has the potential to rank among the most devastating attacks in e-commerce history, comparable to 'Shoplift', 'Ambionics', and 'Trojan Order.

Affected Products

- Adobe Commerce: Versions up to 2.4.7, including 2.4.6-p5, 2.4.5-p7, 2.4.4-p8
- Adobe Commerce Extended Support: Versions up to 2.4.3-ext-7, 2.4.2-ext-7, 2.4.1-ext-7, 2.4.0-ext-7, 2.3.7-p4-ext-7
- Magento Open Source: Versions up to 2.4.7, including 2.4.6-p5, 2.4.5-p7, 2.4.4-p8
- Adobe Commerce Webhooks Plugin: Versions 1.2.0 to 1.4.0

Solution

- Adobe Commerce: 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9

- Adobe Commerce Extended Support: 2.4.3-ext-8, 2.4.2-ext-8, 2.4.1-ext-8, 2.4.0-ext-8, 2.3.7-p4-ext-8
- Magento Open Source: 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9
- Adobe Commerce Webhooks Plugin: 1.5.0

Recommendations

- Immediately update to the patched versions listed above.
- Switch to 'Report-Only' mode before upgrading to avoid checkout functionality issues.
- For those unable to update immediately, check for the vulnerable glibc library using the provided command and upgrade as required.
- Add the emergency fix code to 'app/bootstrap.php' to block most attacks.
- Regularly monitor and apply security updates to ensure protection against new vulnerabilities.

References

- https://www.bleepingcomputer.com/news/security/cosmicsting-flaw-impacts-75-percent-of-adobe-commerce-magento-sites/
- https://helpx.adobe.com/security/products/magento/apsb24-40.html
- https://sansec.io/research/cosmicstinghttps://sansec.io/research/cosmicsting