Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

SessionReaper Flaw Enables Seamless Session Hijacking on Adobe Commerce

Date of Publication	Admiralty Code	TA Number
October 24, 2025	A1	TA2025325

Summary

First Seen: September 2025
Affected Products: Adobe Commerce (including B2B) and Magento Open Source
Impact: The critical SessionReaper (CVE-2025-54236) vulnerability in Adobe Commerce and Magento Open Source, discovered in September 2025, is now under active exploitation. This improper input validation flaw allows unauthenticated attackers to hijack customer accounts and, under certain conditions, achieve remote code execution through the Commerce REST API. Despite Adobe's emergency patch, 62% of Magento stores remain exposed, with over 250 attack attempts recorded in the last 24 hours. Exploits leverage a malicious session injection and nested deserialization bug, echoing the CosmicSting attack pattern, with experts warning of widespread exploitation within 48 hours.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-54236	SessionReaper (Adobe Commerce Improper Input Validation Vulnerability)	Adobe Commerce (including B2B) and Magento Open Source	✗	✓	✓

Vulnerability Details

#1 Hackers are actively exploiting the critical SessionReaper vulnerability, tracked as CVE-2025-54236, which affects Adobe Commerce and Magento Open Source platforms. Discovered in September 2025, this improper input validation flaw enables unauthenticated attackers to hijack customer accounts via the Commerce REST API.

#2 Successful exploitation allows attackers to seize full control of customer sessions and, under specific conditions, execute remote code. The attack requires no user interaction, making it particularly dangerous.

#3 Six weeks after Adobe issued an emergency patch, SessionReaper has entered active exploitation. Despite the patch release, approximately 62% of Magento stores remain unprotected. In the past 24 hours alone, over 250 attack attempts have been detected across multiple stores.

#4 The exploit leverages a malicious session injection combined with a nested deserialization flaw in Magento's REST API. While the confirmed remote code execution path depends on file-based session storage, alternative attack vectors are likely. With technical details now public and active campaigns underway, mass exploitation is expected within 48 hours. The attack mirrors patterns seen in last year's **CosmicSting** incident, signaling a continuation of similar high-impact exploitation trends.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-54236	Adobe Commerce Versions: 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier Adobe Commerce B2B Versions: 1.5.3-alpha2, 1.5.2-p2, 1.4.2-p7, 1.3.4-p14, 1.3.3-p15 and earlier Magento Open Source Versions: 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14 and earlier	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:commerce_b2b:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:magento:-:*:*:open_source:*:*:*	CWE-20

Recommendations

Immediate Patch Deployment: Apply Adobe's emergency patch for CVE-2025-54236 across all Adobe Commerce and Magento Open Source instances without delay. Confirm that all dependencies and extensions are also updated.

Limit public exposure of the Commerce REST API: Implement IP whitelisting, enforce strong authentication, enable request throttling/rate limiting, and apply the principle of least privilege to administrative and API accounts.

Harden perimeter defenses by updating Web Application Firewall rules to include specific signatures and heuristics for SessionReaper payloads and enable intrusion detection to flag malicious session injections and nested deserialization attempts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1210** Exploitation of Remote Services	**T1190** Exploit Public-Facing Application
T1539 Steal Web Session Cookie	**T1211** Exploitation for Defense Evasion	**T1071.001** Web Protocols	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	34[.]227[.]25[.]4, 44[.]212[.]43[.]34, 54[.]205[.]171[.]35, 155[.]117[.]84[.]134, 159[.]89[.]12[.]166

Patch Link

https://helpx.adobe.com/security/products/magento/apsb25-88.html

References

https://experienceleague.adobe.com/en/docs/experience-cloud-kcs/kbarticles/ka-27397

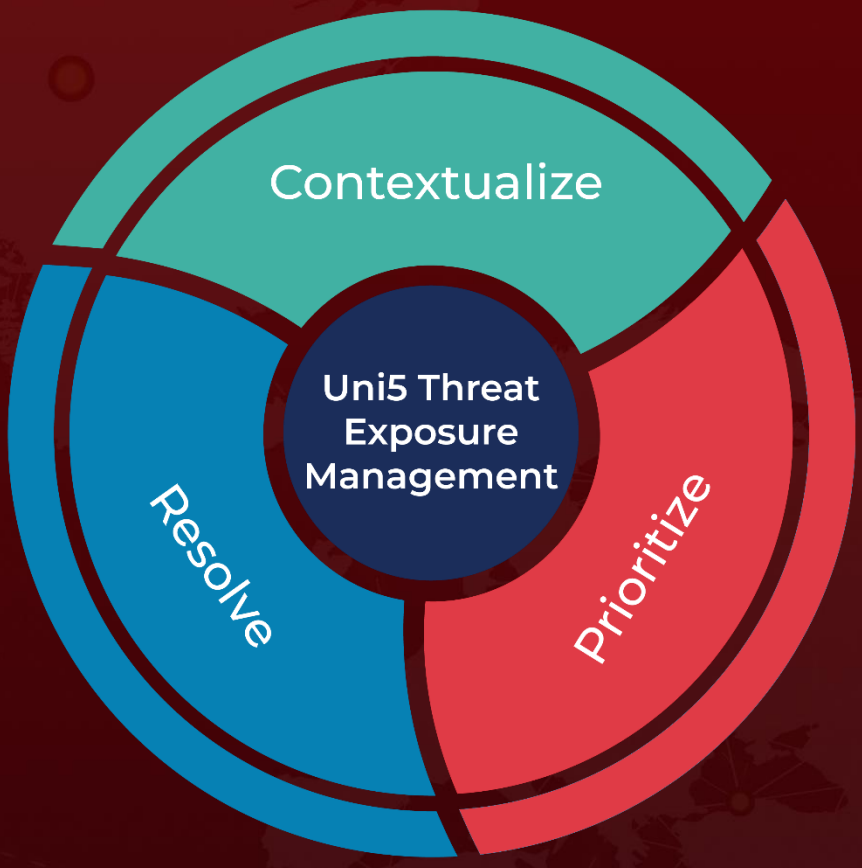
https://sansec.io/research/sessionreaper-exploitation

https://hivepro.com/threat-advisory/wild-exploitation-of-critical-flaw-in-adobe-commerce-and-magento/

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

October 24, 2025 • 07:00 AM

More at www.hivepro.com