

NCA-46.091725 – NCERT Advisory – Critical Adobe Commerce and Magento Vulnerabilities (SessionReaper)

Introduction

A critical vulnerability, tracked as CVE-2025-54236 and nicknamed SessionReaper, has been disclosed in Adobe Commerce and Magento Open Source platforms. The flaw, rated CVSS 9.1 (Critical), arises from improper input validation in the Commerce REST API.

Successful exploitation enables attackers to hijack customer sessions and potentially achieve full account takeover without authentication. Under certain conditions, attackers may also perform remote code execution when file-based session storage is enabled.

This vulnerability impacts multiple Adobe Commerce deployment methods, Magento Open Source, B2B extensions, and the Custom Attributes Serializable Module. Given its severity and similarities to prior major Magento flaws, SessionReaper poses a high risk of customer data compromise, hijacked sessions, and full system takeover.

Impact

Successful exploitation can lead to:

1. **Account Takeover** – Unauthorized access to customer accounts and sensitive data.
2. **Remote Code Execution** – Execution of arbitrary code under specific conditions.
3. **Traffic Interception** – Hijacking of active sessions and interception of transactions.
4. **Privilege Escalation** – Abuse of stolen tokens or API keys.
5. **Service Disruption** – Mass exploitation leading to business downtime.

Threat Details

Vulnerability Overview

- **Incident ID:** SessionReaper – CVE-2025-54236
- **Affected Component:** Adobe Commerce REST API and related modules
- **Description:** Improper input validation in Commerce REST API allows attackers to hijack sessions, bypass authentication, and in some cases execute arbitrary code.

Attack Complexity & Vector

- **Attack Vector:** Remote (via REST API calls)
- **Attack Complexity:** Low
- **Privileges Required:** None (pre-authentication attack)

- **User Interaction:** None required
- **Estimated CVSS v3.1 Score:** 9.1 (Critical)
- **CWE:** CWE-20 (Improper Input Validation), CWE-639 (Authorization Bypass Through User-Controlled Key)

Indicators of Compromise (IoCs)

Category	Indicator / Value	Description / Notes
Suspicious API Activity	Abnormal Commerce REST API requests	Session manipulation or repeated deserialization attempts
Credential Abuse	Repeated login anomalies without credentials	Suggests hijacked sessions
Exploit Behavior	Remote file-based deserialization traffic	Indicator of potential RCE attempt
Admin Access	Unexpected creation of admin/API tokens	Possible exploitation of hijacked session

Exploit Conditions

Exploitation requires:

- Exposure of Commerce REST API to the internet.
- Use of vulnerable Adobe Commerce, B2B, or Magento Open Source versions.
- No patch or hotfix applied.
- In certain cases, file-based session storage enabled (for RCE scenarios).

Affected Versions

- **Adobe Commerce (all deployment methods):** 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
- **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
- **Custom Attributes Serializable Module:** Versions 0.1.0 to 0.4.0

Recommendations & Mitigation Actions

1. Patch Immediately (Recommended Fix)

- Apply emergency hotfix VULN-32437-2-4-X-patch or upgrade to the latest Adobe Commerce / Magento Open Source release (APSB25-88).

- Perform regression testing before deployment to ensure API/deserialization compatibility.
- Rotate administrator credentials and API tokens immediately.

2. Temporary Mitigation (If Patching Not Possible)

- Limit REST API exposure to trusted users and networks only.
- Deploy WAF rules to detect and block malicious API or deserialization traffic.
- Disable unneeded integrations and enforce strict admin/API access controls.
- Monitor for abnormal session or privilege escalation activity.

3. Strengthen Security Posture

- Enforce least privilege principles for API and session handling.
- Regularly audit administrator tokens and integrations.
- Implement continuous anomaly detection on web API activity.

Monitoring & Detection

- Track API calls for unexpected session manipulation.
- Monitor logs for abnormal login activity and privilege escalation attempts.
- Deploy IDS/IPS/WAF signatures for known SessionReaper exploit patterns.
- Alert on unexpected deserialization traffic or unrecognized admin token use.

Patching Summary

Version Category	Components / Modules	Status
Vulnerable	Versions listed under "Affected Versions"	Must patch immediately
Secure	Adobe Commerce / Magento patched to APSB25-88	No action required

References

- [Security update available for Adobe Commerce | APSB25-88](#)
- [SessionReaper, unauthenticated RCE in Magento & Adobe Commerce \(CVE-2025-54236\)](#)

Call to Action

The National CERT advises all organizations running Adobe Commerce or Magento Open Source to:

- Immediately apply the hotfix or upgrade to APSB25-88.
- Rotate all administrator and API credentials.
- Monitor for abnormal REST API and session activity.
- Strengthen WAF, IDS/IPS, and log monitoring to block automated exploitation attempts.

Timely patching is essential to prevent large-scale exploitation of eCommerce platforms.



PKCERT