

Alert Bulletin

Bulletin N.: 98

Publication Date: 08/09/2026

Subject: Alert 2026-98 Critical Zero-Day in Adobe Commerce and Magento Open Source

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fix
Adobe Commerce	2.4.4 2026 aug, 2.4.5 2026 aug, 2.4.6 2026 aug, 2.4.7 2026 aug, 2.4.8 2026 aug, 2.4.9 2026 aug and earlier	Apply VULN 2026 9341 hotfix corresponding to the installed version
Adobe Commerce B2B	1.3.3 2026 aug, 1.3.4 2026 aug, 1.4.2 2026 aug, 1.5.2 2026 aug, 1.5.3 2026 aug and earlier	Apply VULN 2026 9341 hotfix corresponding to the installed version
Magento Open Source	2.4.6 2026 aug, 2.4.7 2026 aug, 2.4.8 2026 aug, 2.4.9 2026 aug and earlier	Apply VULN 2026 9341 hotfix corresponding to the installed version

Adobe officially tested the hotfix on the listed 2026-aug versions. Earlier versions within the affected branches are also vulnerable, but Adobe warns that the patch has not been officially validated on all of those legacy releases; in those cases, it is recommended to first upgrade to a supported version and apply the corresponding hotfix.

Description

Adobe released an emergency update to fix **CVE~~2026~~75650**, a vulnerability of **critical** severity with a **CVSS 10.0** score that allows a remote **unauthenticated** attacker to execute arbitrary code on vulnerable Adobe Commerce and Magento Open Source installations.

The **CVE~~2026~~75650** vulnerability affects the template rendering system of Magento/Adobe Commerce and allows a **Server-Side Template Injection (SSTi)** chain that can result in remote code execution without requiring authentication. The vulnerability is an **improper neutralization of special elements used in a template engine**, classified as **CWE~~2026~~1336**

Sansec's research indicates that the attacker abuses a property called styles within the template mechanism. Through a specially crafted input, they can induce the *dependency injection* system and template processing to instantiate unexpected classes and execute PHP code on the server.

The observed malicious flow uses the creation of an email titled **"Payment Transaction Failed Reminder"** as a vehicle to trigger PHP code injection and cause execution on the server. The unauthenticated access and the ability to execute code make the impact maximum: an attacker can install persistence mechanisms, webshells, malware, steal configuration secrets, access databases, and modify e-commerce logic or payment processes.

Solution

The official solution consists of applying the Adobe hotfix **VULN-39341**, published in bulletin **APSB26-146**, for the specific version of Adobe Commerce, Adobe Commerce B2B, or Magento Open Source deployed. The hotfix fixes the unsafe handling of template values before unintended classes can be instantiated by the rendering engine.

<https://experienceleague.adobe.com/en/docs/commerce-knowledge-base/kb/announcements/commerce-apsb26-146>

Additional information:

- <https://experienceleague.adobe.com/en/docs/commerce-knowledge-base/kb/announcements/commerce-apsb26-146>
- [CVE Program — CVE-2026-75650](#)
- [Sansec — StyleSmuggler: Magento and Adobe Commerce zero-day RCE](#)
- [The Hacker News — Adobe Patches Magento Zero-Day Exploited to Deploy Rust Backdoor and PHP Web Shell](#)