

Traffic Light Protocol (TLP): White

La investigación de Sansec indica que el atacante abusa de una propiedad denominada *styles* dentro del mecanismo de plantillas. Mediante una entrada especialmente diseñada, puede inducir al sistema de *dependency injection* y al procesamiento de plantillas a instanciar clases no esperadas y ejecutar código PHP en el servidor.

El flujo malicioso observado utiliza la creación de un correo denominado **“Payment Transaction Failed Reminder”** como vehículo para activar la inyección de código PHP y disparar la ejecución en el servidor. El acceso no autenticado y la posibilidad de ejecución de código hacen que el impacto sea máximo: un atacante puede instalar persistencia, webshells, malware, robar secretos de configuración, acceder a bases de datos y modificar la lógica de comercio electrónico o los procesos de pago.

Solución

La solución oficial consiste en aplicar el hotfix de Adobe **VULN-39341**, publicado en el boletín **APSB26-146**, para la versión específica de Adobe Commerce, Adobe Commerce B2B o Magento Open Source desplegada. El hotfix corrige el manejo inseguro de valores de plantilla antes de que puedan instanciarse clases no previstas por el motor de renderizado.

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

Información adicional:

- <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](#)