

**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

9 September 2026

**Advisory 273: Adobe Commerce & Magento Open Source Template Engine
Unauthenticated Remote Code Execution — "StyleSmuggler" (CVE-2026-75650).**

Release Date: 8th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and e-commerce or web-development teams that operate an online store on Adobe Commerce, Adobe Commerce B2B, or Magento Open Source. This alert is intended to be understood by both technical users and systems administrators, and requires immediate action given confirmed active exploitation.

What is it?

CVE-2026-75650, codenamed "StyleSmuggler," is a maximum-severity, unauthenticated remote code execution vulnerability in Adobe Commerce, Adobe Commerce B2B, and Magento Open Source - one of the world's most widely-deployed e-commerce platforms and is currently being actively exploited in the wild. The flaw stems from improper sanitisation of GraphQL "styles" template properties (CWE-1336, Improper Neutralization of Special Elements Used in a Template Engine), allowing an unauthenticated attacker to smuggle malicious PHP code into a file that Magento itself writes to disk, then trigger server-side execution by causing the platform's "Payment Transaction Failed Reminder" notification template to render the injected content therefore achieving full remote code execution with no credentials and no user interaction of any kind.

What are the systems affected?

The following version(s) are affected:

- Adobe Commerce 2.4.4 through 2.4.9 (August 2026 builds and earlier) - (Affected)
- Adobe Commerce B2B 1.3.3 through 1.5.3 (August 2026 builds and earlier) - (Affected)
- Magento Open Source 2.4.6 through 2.4.9 (August 2026 builds and earlier) - (Affected)

Apply hotfix VULN-39341 (no incremented version number is issued for this patch) - see "Mitigation process" below.

What does this mean?

Typical attack flow:

1. **Inject malicious PHP into a template-processed store artifact**
 - An unauthenticated attacker abuses improper sanitisation of GraphQL "styles" template properties to smuggle malicious PHP code into a file that Magento itself writes to disk.
2. **Trigger server-side execution via a templated email**
 - By causing the platform's "Payment Transaction Failed Reminder" notification template to render, the previously-smuggled PHP code is executed directly on the server, with no authentication or user interaction required at any stage.

Attack vectors:

- A network-based, unauthenticated attack over HTTP/HTTPS against any internet-facing Adobe Commerce or Magento Open Source storefront exposing GraphQL and templated-notification workflows (admin, email/notification, and GraphQL-related endpoints).
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Achieve full, unauthenticated remote code execution on the affected server, and install a persistent backdoor. This is observed in the wild as a Rust-based Linux implant contacting external command-and-control infrastructure or a PHP web shell for continued arbitrary code execution.
- Access customer data processed by the store, including personal information and payment-related data, and use the compromised server as a foothold to pivot further into the hosting environment.

Indicators of Compromise (IOCs):

Organizations running Adobe Commerce or Magento Open Source should check for the following indicators of compromise, drawn from documented exploitation of this vulnerability:

- Suspicious processes masquerading as legitimate system utilities — "kworker/[...]", "fc-cache", and "chronyd" processes running from unexpected locations.

- Suspicious file paths associated with disguised backdoor binaries: `~/.cache/fontconfig/fc-cache`, `/tmp/.fc-*/fc-cache`, and `/tmp/.chrony-*/chronyd`.
- Unexpected PHP web shells under the `pub/media/` directory, and files containing `"x_trace_"` under `var/report/`.
- Outbound network connections from the web server to unfamiliar external command-and-control infrastructure.

Mitigation process

CERTVU recommends the following:

1. Apply the Adobe hotfix (VULN-39341) immediately. This vulnerability is being actively exploited

- Download and apply patch VULN-39341 from repo.magento.com/patch/VULN-39341-composer-patches.zip per Adobe Security Bulletin APSB26-146, and verify successful application with `"vendor/bin/magento-patches -n status | grep 39341"`.

2. Treat this as a likely-compromise scenario, not just a patch-and-move-on situation. Scan for the indicators of compromise listed above before considering any internet-facing store clean

3. Rotate all credentials and secrets after patching

4. Audit the estate for Adobe Commerce and Magento Open Source deployments

5. Monitor store-facing endpoints and logs for anomalous activity

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-75650>
2. <https://helpx.adobe.com/security/products/magento/psb26-146.html>