Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

StyleSmuggler: Adobe Commerce and Magento Zero-Day Exploited

Date of Publication	Admiralty Code	TA Number
September 07, 2026	A1	TA2026260

Summary

First Seen: September 4, 2026
Affected Products: Adobe Commerce and Magento Open Source, Adobe Commerce on Cloud, Adobe Commerce B2B
Impact: StyleSmuggler, tracked as CVE-2026-75650 (CVSS 10.0), is a template-engine injection flaw in Magento Open Source and Adobe Commerce, exploited in the wild since 4 September 2026, that lets unauthenticated attackers achieve remote code execution by smuggling PHP into a failure report and forcing Magento to execute it while rendering a failed-payment email. Every release from 2.4.4 through 2.4.9 and Adobe Commerce B2B 1.3.3 through 1.5.3 is affected, and fully patched stores were compromised for three days before Adobe released an emergency hotfix on 7 September. Successful attacks install a cron-persisted Rust implant disguised as a kernel thread outside the webroot that evades conventional scanners and reads session data from Redis, so affected organizations must apply the hotfix immediately, hunt for compromise since patching does not remove an existing implant, and rotate the encryption key and every credential it protects.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-75650	StyleSmuggler (Adobe Commerce and Magento Open Source Remote Code Execution Vulnerability)	Adobe Commerce and Magento Open Source, Adobe Commerce B2B	✓	✓	✓

Vulnerability Details

#1

StyleSmuggler is a critical vulnerability in Magento Open Source and Adobe Commerce that allows an unauthenticated remote attacker to execute arbitrary code on the store's server. Tracked as CVE-2026-75650 and rated CVSS 10.0, it was addressed by Adobe through an emergency hotfix on 7 September 2026, with exploitation in the wild confirmed by the vendor. Every release from 2.4.4 through 2.4.9 and Adobe Commerce B2B 1.3.3 through 1.5.3 is affected, and a fully patched 2.4.6-p15 installation carrying the August 2026 update was among the first confirmed victims, so patch level prior to the hotfix offers no protection.

#2

The attack chains two weaknesses in Magento's own code. The attacker first causes Magento to write PHP into a file it can later read, typically a failure report under var/report/ marked with an X_TRACE_ identifier, or alternatively a file uploaded through Magento's product custom options. A crafted template directive abusing style properties then loads that poisoned file through an internal code path intended only for command-line build tasks. Triggering the platform's standard "Payment Transaction Failed Reminder" email executes the payload during rendering, whether or not the message is delivered, giving the attacker code execution as the Magento filesystem user.

#3

Exploitation began on 4 September 2026, the flaw was disclosed on 5 September, and at least two actors are exploiting it, changing payloads several times a day; relocating sessions to Redis or the database is not a mitigation. Successful attacks deploy a self-contained Rust binary with no symbols, built for x86-64 and arm64 in multiple variants, so file hashes vary and signature-based detection has failed. The implant masquerades as the kernel thread [kworker/u:8:0] under a non-root user, installs at ~/.local/share/.gvfsd/gvfsd-user outside the webroot, persists through a cron entry relaunched every five minutes and re-written within a second if removed, beacons to a hardcoded command-and-control server, and on at least one host read session data from local Redis with no outbound traffic.

#4

Organizations should apply Adobe's emergency hotfix immediately and be hunted for compromise, since patching closes the vulnerability but does not remove an implant installed during the three days it was exploited without a fix. Checks should cover the disguised kworker process, the gvfsd cron entry, and X_TRACE_ markers in var/report/. Where the hotfix cannot be applied at once, temporarily disabling GraphQL and restricting PHP process-execution functions reduce exposure, and in all cases the encryption key and every credential it protects should be rotated.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-75650	Adobe Commerce and Magento Open Source 2.4.4 - 2.4.9 (2026-aug and earlier), Adobe Commerce on Cloud, Adobe Commerce B2B 1.3.3 - 1.5.3	cpe:2.3:a:magento:magento:*:*:*:*:open_source:*:*:* cpe:2.3:a:adobe:commerce:*:*:*:*:*:*:*:*	CWE-1336

Recommendations

Apply Adobe's Emergency Hotfix Immediately: Download VULN-39341-composer-patches.zip from repo.magento.com, apply it as a Composer patch, and confirm with vendor/bin/magento-patches -n status | grep "39341\|Status". The hotfix is verified only against 2026-aug patch levels of 2.4.4–2.4.9 and B2B 1.3.3–1.5.3; bring older builds current first. Patching closes the vulnerability but does not clean an existing compromise, so complete the hunt.

Hunt for Compromise in Parallel with Patching: Treat every Magento or Adobe Commerce server that was internet-facing on or after September 4, 2026 as potentially compromised irrespective of patch level, and run these checks whether or not the hotfix has been applied, since patching does not remove an existing implant. Run read-only checks as the Magento filesystem user: list non-root processes whose name begins with a bracket and that hold real resident memory; inspect crontab entries for gvfsd or .kw_; look for ~/.local/share/.gvfsd/, /tmp/.kw_ and /tmp/.gvfsd- files; grep both var/report/ and var/log/ for X_TRACE_ or PHP opening tags; and search web access logs for styles[, styles%5B, generatorClass, with_resolved and cdnflare. Scan the entire user home directory, not just the document root, because the implant installs one level above the webroot and an application-scoped scan has already returned a false clean result.

Follow Evidence-Preserving Containment Order if an Indicator Is Found: Do not reboot, delete the binary, or run composer install first, as each destroys evidence while leaving persistence intact and the copy under /proc/<pid>/exe may be the only remaining binary. Confirm the match, preserve evidence including a hash of the running process from /proc/<pid>/exe, remove the cron entry before stopping the process because the process restores the entry, then remove known files, and hunt for secondary persistence in systemd timers, other cron locations, shell profiles, SSH keys, PHP configuration, admin accounts, API integrations and CMS content. Wait more than one five-minute cron cycle and repeat the checks.

Monitor Failed-Payment Emails and Access Logs as Early Warning: Investigate any unexpected burst of Payment Transaction Failed Reminder emails, and treat a notice containing unresolved template variables, a .invalid customer domain, a zero order total or the error-generating-content fallback text as exploitation exhaust. A TypeError from array_merge() in system.log immediately after an include indicates the payload already executed, although a stealthier variant returns an empty array and leaves no log trace.

Rotate Every Credential the Application Could Read and Flush Sessions: Because the implant read Magento session storage from Redis, invalidate all sessions and flush session storage, then rotate the crypt/key in app/etc/env.php, every administrator password, every payment-provider API key, database credentials, and every other integration credential held in that file. Adobe's rotation guidance additionally covers REST, SOAP and GraphQL integration tokens, OAuth client secrets, SSH and deploy keys, and third-party extension API keys.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1053: Scheduled Task/Job	T1053.003: Cron
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1027: Obfuscated Files or Information	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Collection	T1005: Data from Local System	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e315687a1dfe61ef4a5a5642214db6d3b2b05d81391285eebc2af664641a26a7, b79dfdc1eed860e0b76c629d6adfce251db379b0b45a6d728d4ef483f7551420, 4352cabaa451e5a894535fbcc4d46628701303322a13745cb5479d7d0534ae8e, d2fbf9eb75c495bfea48790d3b228fab0c15a282419c3d3f5e49294c4e1a3e82, 1a3374ffac5b0a62467612f264c49792d206304d4514409c982325c91231375d, 8334b434fa3fe9f59cebe9609b11e0b1fd19d10212c45c705adec1902a1d06ef, 251fabd50d7b18a8b5e1b3ef5d64e7198c17244778f6461fb1ab07f6169bf220, d61217ca0bca83204302fa7b41935ce36f73764559c156d5c980f2fedddffb6e
Domain	247[.]cdnflare[.]xyz, windwsecurity[.]run, ntp[.]timesysnc[.]net, time[.]microsft[.]run, pool[.]microsft[.]studio, ntp[.]timesync[.]to, ntp[.]synctime[.]to, ntp[.]syncstime[.]to, 457cfa2fb7p5[.]daf892t5qau4og8pi4cghbc6fhm1dim3u[.]oast[.]site
URL	hxxps[:]//www[.]incofar[.]it/js/jquery/plugins/ajaxfileupload/mag[.]txt
IPv4:Port	99[.]84[.]67[.]186[:]443, 185[.]157[.]160[.]251[:]123
IPv4	209[.]141[.]43[.]95, 88[.]216[.]72[.]181, 182[.]182[.]152[.]48, 76[.]31[.]99[.]207, 209[.]73[.]130[.]148, 77[.]239[.]124[.]107, 5[.]181[.]86[.]133, 91[.]238[.]181[.]19
IPv6	2a06[:]98c1[:]3120[::]2, 2a06[:]98c1[:]3121[::]2

TYPE	VALUE
Filename	gvfsd-user, fc-cache, chronyd, kworker-linux-x64, kworker-linux-arm64
File Path	~/.local/share/.gvfsd/gvfsd-user, ~/.local/share/.gvfsd/.gvfsd_<8hex>.lock, ~/.cache/fontconfig/fc-cache, /tmp/.kw_<random><random>, /tmp/.cache_<random><random>, /tmp/.fc-<8hex>/fc-cache, /tmp/fc-cache, /tmp/.fc_<8hex>.lock, /tmp/.chrony-<8hex>/chronyd, pub/media/catalog/product/cache/ss_<10hex>/sync_<10hex>.php, var/report/, var/log/system.log
Process Name	[kworker/u:8:0], fc-cache, chronyd
Cron Entry	*/5 * * * * exec <home>/.local/share/.gvfsd/gvfsd-user, */5 * * * * exec /tmp/.kw_<random><random>, 13,43 * * * * <home>/.cache/fontconfig/fc-cache >/dev/null 2>&1, 57,27 * * * * /tmp/.chrony-<8hex>/chronyd >/dev/null 2>&1
HTTP Request	POST /graphql?styles[...]=, POST /paypal/transparent/response/?<?=eval(base64_decode('..., GET /customer/section/load/?sections=customer&force_new_section_timestamp=true, POST /graphql, body {"query":"query { storeConfig { store_code } }"}, PHP in Store: header, X-TRACE-<10hex>, X-<12hex>, X-Cache-Token: fced27f6d57702565353ecc11722533b
User-Agent	python-requests 2.15.0, python-requests/2.32.4, Mozilla/5.0
Log Artifact	MG<20hex>::<base64>::/MG<20hex>, crontab command not allowed, ss5_457cfa2fb7, ss6_457cfa2fb7_, 457cfa2fb7d<n>-<chunk>.daf892t5qau4og8pi4cghbc6fhm1dim3u.oast.site

Patch Links

https://helpx.adobe.com/security/products/magento/apsb26-146.html

https://helpx.adobe.com/security/products/magento.html

References

https://sansec.io/research/stylesmuggler

https://www.disrex.nl/blogs/stylesmuggler-magento-zero-day

https://helpx.adobe.com/security/products/magento/apsb26-146.html

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 Demo of **HivePro**.

REPORT GENERATED ON

September 07, 2026 • 11:45 PM

More at www.hivepro.com