

CVE-2026-48356

Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability

Exigent

CISA KEV since Oct 27, 2026

Actively exploited

Adobe Commerce is affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.

EVRS

85/100

Immediate priority

CVSS V3.1

9.3

Critical · NVD

EPSS

0.306

98.2nd percentile · FIRST

CISA DEADLINE

Nov 10, 2026

CISA federal deadline in 13 days

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 30 days
☒ EPSS	0.306 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
commerce	2.4.4	no fixed version listed	NVD
	2.4.5		
	2.4.6		
	2.4.7		
	2.4.8		
	2.4.9		
commerce b2b	1.3.3	no fixed version listed	NVD
	1.3.4		
	1.4.2		
	1.5.2		
	1.5.3		
magento	2.4.6	no fixed version listed	NVD
	2.4.7		
	2.4.8		
	2.4.9		
i\o events	≥ 1.6.0 < 1.21.0	1.21.0	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-p3ch-8535-fp8j	Additional guidance	helpx.adobe.com/security/products/magento/apsb26-73.html
adobe.com	adobe.com/trust/security/products/commerce/apsb26-73.html	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-48356
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-44420
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-48356		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.