

CVE-2022-24086

Adobe Commerce and Magento Open Source Improper Input Validation Vulnerability

Exigent

CISA KEV since Feb 15, 2022

Actively exploited

Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. Exploitation of this issue does not require user interaction and could result in arbitrary code execution.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.992 99.94th percentile · FIRST	CISA DEADLINE Mar 1, 2022 KEV since 2022 · listed over a year
--	--	---	---

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	On the CISA KEV catalog for over two years
☒ EPSS	0.992 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
commerce	$< 2.3.0$ $\geq 2.3.3 \leq 2.3.6$ $\geq 2.4.0 \leq 2.4.2$ 2.3.7 2.4.3	2.3.0 · after 2.3.6 · after 2.4.2	NVD
magento	$< 2.3.0$ $> 2.3.3 \leq 2.3.6$ $\geq 2.4.0 \leq 2.4.2$ 2.3.7 2.4.3	2.3.0 · after 2.3.6 · after 2.4.2	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/magento/apsb22-12.html	NVD	nvd.nist.gov/vuln/detail/CVE-2022-24086
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2022-0975
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-24086		

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