



CVE-2023-29291

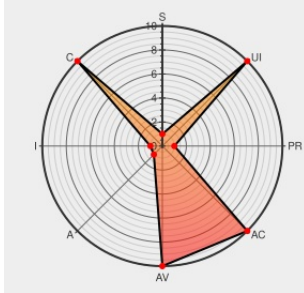
Published on: Not Yet Published

Last Modified on: 06/22/2023 03:41:00 PM UTC

CVE-2023-29291

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Commerce](#) from [Adobe](#) contain the following vulnerability:

Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs.

Exploitation of this issue does not require user interaction.

CVE-2023-29291 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Adobe - Magento Commerce** version <= 2.4.6

Affected Vendor/Software: **Adobe - Magento Commerce** version <= 2.4.5-p2

Affected Vendor/Software: **Adobe - Magento Commerce** version <= 2.4.4-p3

Affected Vendor/Software: **Adobe - Magento Commerce** version <= None

CVSS3 Score: **4.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Adobe Security Bulletin	helpx.adobe.com text/html	MISC helpx.adobe.com/security/products/magento/apsb23-35.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Commerce	2.3.7	-	All	All
Application	Adobe	Commerce	2.3.7	p1	All	All
Application	Adobe	Commerce	2.3.7	p2	All	All
Application	Adobe	Commerce	2.3.7	p3	All	All
Application	Adobe	Commerce	2.3.7	p4	All	All
Application	Adobe	Commerce	2.3.7	p4-ext1	All	All
Application	Adobe	Commerce	2.3.7	p4-ext2	All	All
Application	Adobe	Commerce	2.4.0	-	All	All
Application	Adobe	Commerce	2.4.0	ext-1	All	All
Application	Adobe	Commerce	2.4.0	ext-2	All	All
Application	Adobe	Commerce	2.4.1	-	All	All
Application	Adobe	Commerce	2.4.1	ext-1	All	All
Application	Adobe	Commerce	2.4.1	ext-2	All	All
Application	Adobe	Commerce	2.4.2	-	All	All
Application	Adobe	Commerce	2.4.2	ext-1	All	All
Application	Adobe	Commerce	2.4.2	ext-2	All	All
Application	Adobe	Commerce	2.4.3	-	All	All
Application	Adobe	Commerce	2.4.3	ext-1	All	All
Application	Adobe	Commerce	2.4.3	ext-2	All	All
Application	Adobe	Commerce	2.4.4	-	All	All
Application	Adobe	Commerce	2.4.4	p1	All	All
Application	Adobe	Commerce	2.4.4	p2	All	All
Application	Adobe	Commerce	2.4.4	p3	All	All
Application	Adobe	Commerce	2.4.5	-	All	All
Application	Adobe	Commerce	2.4.5	p1	All	All
Application	Adobe	Commerce	2.4.5	p2	All	All
Application	Adobe	Commerce	2.4.6	-	All	All
Application	Adobe	Magento	2.4.4	-	All	All

Application	Adobe	Magento	2.4.4	p1	All	All
Application	Adobe	Magento	2.4.4	p2	All	All
Application	Adobe	Magento	2.4.4	p3	All	All
Application	Adobe	Magento	2.4.5	-	All	All
Application	Adobe	Magento	2.4.5	p1	All	All
Application	Adobe	Magento	2.4.5	p2	All	All
Application	Adobe	Magento	2.4.6	-	All	All
cpe:2.3:a:adobe:commerce:2.3.7:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p3:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p4:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p4-ext1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.3.7:p4-ext2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.0:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.0:ext-1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.0:ext-2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.1:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.1:ext-1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.1:ext-2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.2:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.2:ext-1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.2:ext-2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.3:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.3:ext-1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.3:ext-2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.4:-:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.4:p1:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.4:p2:*:*:*:*:						
cpe:2.3:a:adobe:commerce:2.4.4:p3:*:*:*:*:						

cpe:2.3:a:adobe:commerce:2.4.5:-:*:*:*:*:*:
cpe:2.3:a:adobe:commerce:2.4.5:p1:*:*:*:*:*:
cpe:2.3:a:adobe:commerce:2.4.5:p2:*:*:*:*:*:
cpe:2.3:a:adobe:commerce:2.4.6:-:*:*:*:*:*:
cpe:2.3:a:adobe:magento:2.4.4:-:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.4:p1:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.4:p2:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.4:p3:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.5:-:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.5:p1:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.5:p2:*:*:open_source:*:*:*:
cpe:2.3:a:adobe:magento:2.4.6:-:*:*:open_source:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-29291 : Adobe Commerce versions 2.4.6 and earlier , 2.4.5-p2 and earlier and 2.4.4-p3 and earlier are... twitter.com/i/web/status/1...	2023-06-15 19:16:24
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2023-06-14 12:53:17