

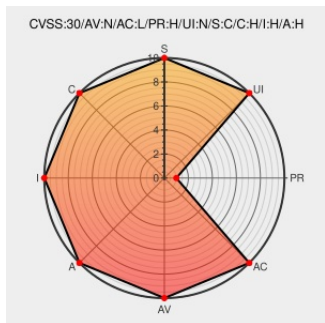


CVE-2021-21014

Published on: 02/11/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:59 PM UTC

CVE-2021-21014

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

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

Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to a file upload restriction bypass. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.

CVE-2021-21014 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: Adobe - **Magento Commerce** version <= 2.4.1

Affected Vendor/Software: Adobe - **Magento Commerce** version <= 2.4.0-p1

Affected Vendor/Software: Adobe - **Magento Commerce** version <= 2.3.6

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

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Adobe Security Bulletin	Vendor Advisory helpx.adobe.com text/html	 MISC helpx.adobe.com/security/products/magento/apsb21-08.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

Exploit/POC from Github

Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to a file upload ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Magento	Magento	All	All	All	All
Application	Magento	Magento	All	All	All	All
Application	Magento	Magento	2.3.6	-	All	All
Application	Magento	Magento	2.3.6	-	All	All
Application	Magento	Magento	2.4.0	-	All	All
Application	Magento	Magento	2.4.0	-	All	All
Application	Magento	Magento	2.4.0	p1	All	All
Application	Magento	Magento	2.4.0	p1	All	All
Application	Magento	Magento	2.4.1	-	All	All
Application	Magento	Magento	2.4.1	-	All	All
Application	Magento	Magento	All	All	All	All
Application	Magento	Magento	All	All	All	All
Application	Magento	Magento	2.3.6	-	All	All
Application	Magento	Magento	2.3.6	-	All	All
Application	Magento	Magento	2.4.0	-	All	All
Application	Magento	Magento	2.4.0	-	All	All
Application	Magento	Magento	2.4.0	p1	All	All
Application	Magento	Magento	2.4.0	p1	All	All
Application	Magento	Magento	2.4.1	-	All	All

Application	Magento	Magento	2.4.1	-	All	All
cpe:2.3:a:magento:magento:*:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:*:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.3.6:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.3.6:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.0:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.0:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.0:p1:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.0:p1:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.1:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.1:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:*:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:*:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.3.6:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.3.6:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.0:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.0:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.0:p1:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.0:p1:*:*:open_source:*:*:						
cpe:2.3:a:magento:magento:2.4.1:*:*:commerce:*:*:						
cpe:2.3:a:magento:magento:2.4.1:*:*:open_source:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report