

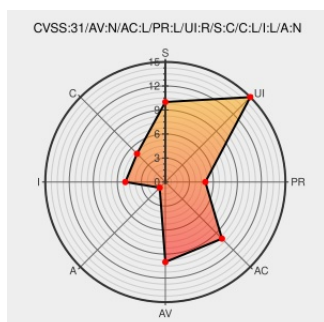


CVE-2022-44470

Published on: Not Yet Published

Last Modified on: 01/06/2023 08:31:00 PM UTC

CVE-2022-44470

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

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

Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.

CVE-2022-44470 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Adobe - Experience Manager** version <= 6.5.14.0

Affected Vendor/Software: **Adobe - Experience Manager** version <= None

Affected Vendor/Software: **Adobe - Experience Manager** version <= None

Affected Vendor/Software: **Adobe - Experience Manager** version <= None

CVSS3 Score: **5.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Adobe Security Bulletin	helpx.adobe.com text/html	MISC helpx.adobe.com/security/products/experience-manager/apsb22-59.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

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

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Experience Manager	All	All	All	All
Application	Adobe	Experience Manager Cloud Service	All	All	All	All
cpe:2.3:a:adobe:experience_manager:*.***.***.***:.*						
cpe:2.3:a:adobe:experience_manager_cloud_service:*.***.***.***:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-44470 : Adobe Experience Manager version 6.5.14 and earlier is affected by a reflected Cross-Site Script... twitter.com/i/web/status/1...	2022-12-19 20:13:49
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution - PATCH NOW	2022-12-14 14:09:32
 /r/netcve	CVE-2022-44470	2022-12-19 21:41:05

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)