

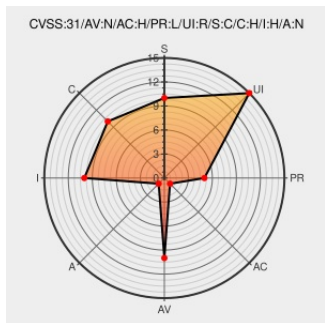


CVE-2021-21379

Published on: 03/12/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:58 PM UTC

CVE-2021-21379 - advisory for GHSA-v662-xpcc-9xf6

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

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

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions of XWiki Platform, the `{{wikimacrocontent}}` executes the content with the rights of the wiki macro author instead of the caller of that wiki macro. This makes possible to inject scripts through it and they will be executed with the rights of the wiki macro (very often a user which has Programming

rights). Fortunately, no such macro exists by default in XWiki Standard but one could have been created or installed with an extension. This vulnerability has been patched in versions XWiki 12.6.3, 11.10.11 and 12.8-rc-1. There is no easy workaround other than disabling the affected macros. Inserting content in a safe way or knowing what is the user who called the wiki macro is not easy.

CVE-2021-21379 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **xwiki - xwiki-platform** version **>= 11.4.0, < 11.10.11**

Affected Vendor/Software: **xwiki - xwiki-platform** version **>= 12.0.0, < 12.6.3**

Affected Vendor/Software: **xwiki - xwiki-platform** version **>= 12.7.0, < 12.8-rc-1**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
It's possible to execute anything with the rights of the author of a macro which uses the {{wikimacrocontent}} macro · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	 CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-v662-xpcc-9xf6
[XWIKI-17759] {{wikimacrocontent}} macro executes the content with the wrong author - XWiki.org JIRA	jira.xwiki.org text/html	 MISC jira.xwiki.org/browse/XWIKI-17759

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.

Related QID Numbers

983847 Java (maven) Security Update for org.xwiki.platform:xwiki-platform-rendering-wikimacro-store (GHSA-v662-xpcc-9xf6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xwiki	Xwiki	All	All	All	All
Application	Xwiki	Xwiki	All	All	All	All

cpe:2.3:a:xwiki:xwiki:*****:.*