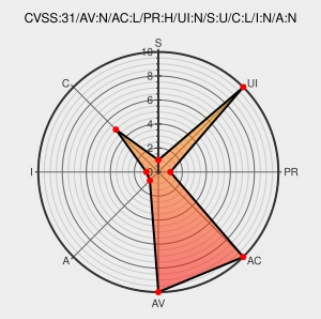
CVE-2022-29253

Published on: Not Yet Published

Last Modified on: 06/07/2022 07:48:00 PM UTC

CVE-2022-29253 - advisory for GHSA-9qrp-h7fw-42hg

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. Starting with version 8.3-rc-1 and prior to versions 12.10.3 and 14.0, one can ask for any file located in the classloader using the template API and a path with ".." in it. The issue is patched in versions 14.0 and 13.10.3. There is no easy workaround for this issue.

CVE-2022-29253 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 8.3-rc-1, < 13.10.3**

CVSS3 Score: 2.7 - LOW

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[XWIKI-19349] It's possible to access a classloader file	jira.xwiki.org	MISC jira.xwiki.org/browse/XWIKI-19349

out of the "templates/" prefix through template manager - XWiki.org JIRA	text/html	
It's possible to access a classloader file out of the "templates/" prefix through template manager · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-9qrp-h7fw-42hg
XWIKI-19349: Bad handling of classloader templates path resolution · xwiki/xwiki-platform@4917c8f · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/4917c8f355717bb636d763844528b1fe0f95e8e2

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	Xwiki	Xwiki	All	All	All	All
Application	Xwiki	Xwiki	8.3	rc1	All	All

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

cpe:2.3:a:xwiki:xwiki:8.3:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29253 : XWiki Platform is a generic wiki platform offering runtime services for applications built on top… twitter.com/i/web/status/1…	2022-05-25 20:59:50
@LinInfoSec	Xwiki - CVE-2022-29253: github.com/xwiki/xwiki-pl…	2022-05-25 23:02:06
/r/netcve	CVE-2022-29253	2022-05-25 21:38:57

← Previous ID Next ID→