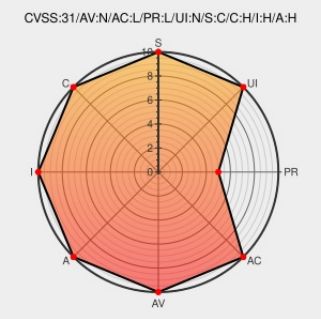
CVE-2022-41934

Published on: Not Yet Published

Last Modified on: 11/23/2022 08:41:00 PM UTC

CVE-2022-41934 - advisory for GHSA-6w8h-26xx-cf8q

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xwiki-platform from Xwiki contain the following vulnerability:

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights on commonly accessible documents including the menu macro can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation due to improper escaping of the macro content and parameters of the menu macro. The problem has been patched in XWiki 14.6RC1, 13.10.8 and 14.4.3. The patch (commit `2fc20891`) for the document `Menu.MenuMacro` can be manually applied or a XAR archive of a patched version can be imported. The menu macro was basically unchanged since XWiki 11.6 so on XWiki 11.6 or later the patch for version of 13.10.8 (commit `59ccca24a`) can most likely be applied, on XWiki version 14.0 and later the versions in XWiki 14.6 and 14.4.3 should be appropriate.

CVE-2022-41934 has been assigned by security-advisories@github.com to track the vulnerability

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **< 13.10.8**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 14.0.0, < 14.4.3**

CVE References

Description	Tags	Link
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in org.xwiki.platform:xwiki-platform-menu-ui · Advisory · xwiki/xwiki-platform · GitHub	github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-6w8h-26xx-cf8q
XWIKI-19857: Modernize the menu macro and add escaping · xwiki/xwiki-	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/2fc20891e6c6b0ca05ee07e315e7f435e8919f8d

platform@2fc2089 · GitHub		
XWIKI-19857: Modernize the menu macro and add escaping · xwiki/xwiki-platform@59ccca2 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-platform/commit/59ccca24a8465a19f40c51d65fcc2c09c1edea16
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-19857
Imports (XWiki.org)	www.xwiki.org text/html	MISC www.xwiki.org/xwiki/bin/view/Documentation/UserGuide/Features/Imports#HImportingXWikipages

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 Software

Vendor	Product	Version
Xwiki	xwiki-platform	< 13.10.8
Xwiki	xwiki-platform	>= 14.0.0, < 14.4.3

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-41934	2022-11-23 20:38:45

← Previous ID

Next ID→