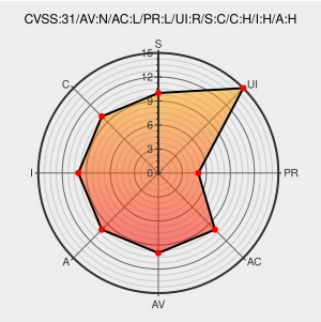
CVE-2023-29201

Published on: Not Yet Published

Last Modified on: 04/25/2023 06:26:00 PM UTC

CVE-2023-29201 - advisory for GHSA-m3jr-cvhj-f35j

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



Certain versions of Xwiki from Xwiki contain the following vulnerability:

XWiki Commons are technical libraries common to several other top level XWiki projects. The "restricted" mode of the HTML cleaner in XWiki, introduced in version 4.2-milestone-1, only escaped `<script>` and `<style>`-tags but neither attributes that can be used to inject scripts nor other dangerous HTML tags like `<iframe>`. As a consequence, any code relying on this "restricted" mode for security is vulnerable to JavaScript injection ("cross-site scripting"/XSS). When a privileged user with programming rights visits such a comment in XWiki, the malicious JavaScript code is executed in the context of the user session. This allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. This problem has been patched in XWiki 14.6 RC1 with the introduction of a filter with allowed HTML elements and attributes that is enabled in restricted mode. There are no known workarounds apart from upgrading to a version including the fix.

CVE-2023-29201 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **xwiki** - **xwiki-commons** version **= >= 4.2-milestone-1, < 14.6-rc-1**

CVSS3 Score: 9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link

XCOMMONS-2426: Provide a component for filtering safe HTML elements a… · xwiki/xwiki-commons@4a185e0 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-commons/commit/4a185e0594d90cd4916d60aa60bb4333dc5623b2
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XWIKI-9118
[XCOMMONS-1680] Filter Html attributes in restricted mode based on a whitelist - XWiki.org JIRA	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XCOMMONS-1680
Loading...	jira.xwiki.org text/html	MISC jira.xwiki.org/browse/XCOMMONS-2426
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in org.xwiki.commons:xwiki-commons-xml · Advisory · xwiki/xwiki-commons · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-commons/security/advisories/GHSA-m3jr-cvhj-f35j
XCOMMONS-1680: Filter Html attributes in restricted mode based on a w… · xwiki/xwiki-commons@b11eae9 · GitHub	github.com text/html	MISC github.com/xwiki/xwiki-commons/commit/b11eae9d82cb53f32962056b5faa73f3720c6182

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← 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 registred 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