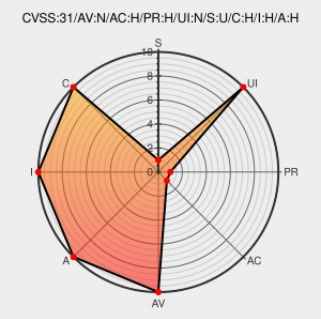
CVE-2020-15171

Published on: 09/10/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:49:00 PM UTC

CVE-2020-15171 - advisory for GHSA-7qw5-pqhc-xm4g

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



Certain versions of Xwiki from Xwiki contain the following vulnerability:

In XWiki before versions 11.10.5 or 12.2.1, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that may lead to arbitrary code execution. The only workaround is to give SCRIPT right only to trusted users.

CVE-2020-15171 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **<11.10.5**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>=12.0.0, <12.2.1**

CVSS3 Score: 6.6 - MEDIUM

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Users with SCRIPT right can access the application server instance manager and create arbitrary Java objects through $request binding · Advisory · xwiki/xwiki-platform · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/xwiki/xwiki-platform/security/advisories/GHSA-7qw5-pqhc-xm4g

Related QID Numbers

983501 Java (maven) Security Update for org.xwiki.platform:xwiki-platform-oldcore (GHSA-7qw5-pqhc-xm4g)

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:*:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Xwiki - CVE-2020-15171: github.com/xwiki/xwiki-pl…	2021-11-18 21:46:13

← Previous ID

Next ID→