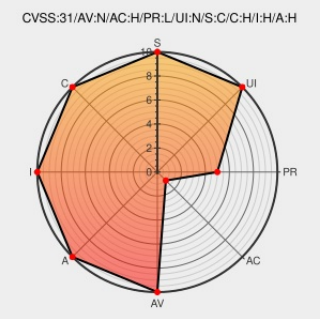
# CVE-2020-15252

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:16:00 PM UTC

## CVE-2020-15252 - advisory for GHSA-5hv6-mh8q-q9v8

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




Certain versions of Xwiki from Xwiki contain the following vulnerability:

In XWiki before version 12.5 and 11.10.6, 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. This is patched in XWiki 12.5 and XWiki 11.10.6.

CVE-2020-15252 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **>= 12.0, < 12.5**

Affected Vendor/Software: **xwiki** - **xwiki-platform** version **< 11.10.6**

### CVSS3 Score: 8.8 - HIGH

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

### CVSS2 Score: 9 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| [XWIKI-17141] Server-Side Template Injection (Velocity) - XWiki.org JIRA | Exploit<br>Vendor Advisory<br>jira.xwiki.org<br>text/html | MISC<br>jira.xwiki.org/browse/XWIKI-17141 |
| Users with SCRIPT right can access the application server instance manager and create arbitrary Java objects through $xcontext.request and $context.request binding · Advisory · xwiki/xwiki-platform · GitHub | Third Party Advisory<br>github.com<br>text/html | CONFIRM<br>github.com/xwiki/xwiki-platform/security/advisories/GHSA-5hv6-mh8q-q9v8 |
| [XWIKI-17423] It's possible to access the ServletContext through Context#getRequest - XWiki.org JIRA | Vendor Advisory<br>jira.xwiki.org<br>text/html | MISC<br>jira.xwiki.org/browse/XWIKI-17423 |



## Related QID Numbers

983502 Java (maven) Security Update for org.xwiki.platform:xwiki-platform-oldcore (GHSA-5hv6-mh8q-q9v8)

## 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) |
|---|---|---|

← Previous ID  Next ID→