Remote code execution with script right through unprotected Velocity scripting API

High **michitux** published **GHSA-h259-74h5-4rh9** 2 days ago

Package

org.xwiki.platform:xwiki-platform-legacy-oldcore (Maven)

Affected versions	Patched versions
>= 17.0.0-rc-1, < 17.4.8	17.4.8
>= 17.5.0-rc-1, < 17.10.1	17.10.1

org.xwiki.platform:xwiki-platform-oldcore (Maven)

>= 17.0.0-rc-1, < 17.4.8	17.4.8
>= 17.5.0-rc-1, < 17.10.1	17.10.1

Description

Impact

An improperly protected scripting API allows any user with script right to bypass the sandboxing of the Velocity scripting API and execute, e.g., arbitrary Python scripts, allowing full access to the XWiki instance and thereby compromising the confidentiality, integrity and availability of the whole instance. Note that script right already constitutes a high level of access that we don't recommend giving to untrusted users.

Patches

The vulnerability has been patched in XWiki 17.4.8 and 17.10.1 by requiring programming right to access the affected scripting API.

Workarounds

We're not aware of any workarounds except for being careful whom you grant script right.

References

- https://jira.xwiki.org/browse/XWIKI-23698
- https://jira.xwiki.org/browse/XWIKI-23702
- `9fe84da`

Attribution

We thank Youssef Azefzaf for discovering and reporting this vulnerability.

Severity

High 8.6 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	High
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-33229

Weaknesses

▶ CWE-862

Credits

azefzafyoussef Reporter