Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in xwiki-platform-wiki-ui-mainwiki

Critical **surli** published **GHSA-xr6m-2p4m-jvqf** on Sep 8

Package

xwiki-platform-wiki-ui-mainwiki (Maven)

Affected versions	Patched versions
>=5.3-milestone-2	13.10.6,14.4

Description

Impact

It's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the request (URL parameter) using the `XWikiServerClassSheet` if the user has view access to this sheet and another page that has been saved with programming rights, a standard condition on a public read-only XWiki installation or a private XWiki installation where the user has an account. This allows arbitrary Groovy/Python/Velocity code execution which allows bypassing all rights checks and thus both modification and disclosure of all content stored in the XWiki installation. Also, this could be used to impact the availability of the wiki.

On current versions (e.g., 14.3), this can be triggered by opening the URL `/xwiki/bin/view/Main/?sheet=XWiki.XWikiServerClassSheet&form_token=<form_token>&action=delete&domain=foo%22%2F%7D%7D%7B%7Basync%20async%3D%22true%22%20cached%3D%22false%22%20context%3D%22doc.reference%22%7D%7D%7B%7Bgroovy%7D%7Dprintln(%22hello%20from%20groovy!%22)%7B%7B%2Fgroovy%7D%7D%7B%7B%2Fasync%7D%7D` , on version 5.3 Milestone 2 (oldest impacted version), the issue can be reproduced using `<server>/xwiki/bin/view/Main/?sheet=WikiManager.XWikiServerClassSheet&form_token=<form_token>&action=delete&domain=foo%22%2F%7D%7D%7B%7B%2Ferror%7D%7D%7B%7B%2Fhtml%7D%7D%7B%7Bfootnote%7D%7D%7B%7Bgroovy%7D%7Dprintln%28%22hello+from+groovy%21%22%29%7B%7B%2Fgroovy%7D%7D%7B%7B%2Ffootnote%7D%7D` . In both cases `<server>` is the URL of the XWiki installation and `<form_token>` is the token used for CSRF protection for the current user which is available in every HTML response (search for `form-token` or `form_token` in the HTML source). If the string `hello from groovy` without `println("` before it is displayed, the attack has been successful.

Patches

This has been patched in the supported versions 13.10.6 and 14.4.

Workarounds

It is possible to edit the affected document `XWiki.XWikiServerClassSheet` or `WikiManager.XWikiServerClassSheet` and manually perform the changes from the patch fixing the issue, i.e., replacing

```
      {{error}}{{translation key="platform.wiki.sheet.erroraliasalreadynotexists"
  parameters="$request.domain"/}}{{/error}}
```

by

```
      {{error}}{{translation key="platform.wiki.sheet.erroraliasalreadynotexists"
  parameters="~"${services.rendering.escape($escapetool.java($request.domain),
  'xwiki/2.1')}~""/}}{{/error}}
```

and replacing

```
      {{error}}{{translation key="platform.wiki.sheet.erroraliasdoesnotexists"
  parameters="$request.domain"/}}{{/error}}
```

by

```
      {{error}}{{translation key="platform.wiki.sheet.erroraliasdoesnotexists"
  parameters="~"${services.rendering.escape($escapetool.java($request.domain),
  'xwiki/2.1')}~""/}}{{/error}}
```

Note that below version 7.1 milestone 1, the used escaping function isn't available and thus a different fix would need to be developed.

On XWiki versions 12.0 and later, it is also possible to import the document `XWiki.XWikiServerClassSheet` from the xwiki-platform-wiki-ui-mainwiki package version 14.4 using the import feature of the administration application as there have been no other changes to this document since XWiki 12.0.

References

- `fc77f9f`
- https://jira.xwiki.org/browse/XWIKI-19746

For more information

If you have any questions or comments about this advisory:

- Open an issue in Jira XWiki.org
- Email us at Security Mailing List

Severity

Critical 9.9 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE ID

CVE-2022-36099

Weaknesses

CWE-95