Cross-site Scripting (XSS) - Stored in forkcms/forkcms

0

Valid Reported on Oct 25th 2021

Description

When uploading a new module, the description of the module can contain JavaScript code. After uploading the new module and looking at the `Details` page, the JavaScript code would be executed.

Proof of Concept

I downloaded this module

```
https://github.com/friends-of-forkcms/fork-cms-module-banners/archive/maste
```

, unzipped it and adjusted the `description` path of the file

```
src/Backend/Modules/Banners/info.xml
```

to this

```
<description>
    <![CDATA[
        The banners module.
        <script>alert(4);</script>
    ]]>
</description>
```

After adjusting the `info.xml` file, pack all files back to a zip file and upload it as new module. After upload, visit the Details page of this module.

Impact

Impact

Executing any JavaScript an attacker could think of. By default, it is used to steal session cookies.

CVE
CVE-2022-0145
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

starkitsec
@starkitsec
unranked

Fixed by

Jelmer Prins
@carakas
maintainer

This report was seen 411 times.

We have contacted a member of the **forkcms** team and are waiting to hear back a year ago

We have sent a follow up to the **forkcms** team. We will try again in 7 days. a year ago

We have sent a second follow up to the **forkcms** team. We will try again in 10 days. a year ago

We have sent a third and final follow up to the **forkcms** team. This report is stale. a year ago

Jelmer Prins validated this vulnerability a year ago

starkitsec has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Jelmer Prins 8 months ago Maintainer

fix is currently in review

Jelmer Prins marked this as fixed in 5.11.1 with commit 981730 8 months ago

Jelmer Prins has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation