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

0

Valid Reported on Mar 23rd 2021

✍️ Description

A cross-site scripting (XSS) issue in the Fork version 5.9.3 allows remote attackers to inject JavaScript via the "publish_on_date" Parameter

🦹‍♂️ Proof of Concept

Vulnerable parameter: publish_on_date
XSS payload: '"()%26%25<yes><ScRiPt%20>alert(1)</ScRiPt>

Steps to reproduce issue

1- Login to Fork admin panel
2- Goto Modules=>Blog=>Edit
3- Turn on Burp Intercept
4- Click on "Publish"
5- Change value of "publish_on_date" parameter to 22/03/2021'"()&%<yes><ScRiPt >alert(2)</ScRiPt>
6- Forward the request and XSS will be triggered

Video POC: https://drive.google.com/file/d/10e_8aSNUsGolDDexhuN_aqso5VA8671n/view?usp=sharing.

```
# 💥 Impact
With the help of xss attacker can perform social engineering on users by re
```

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

Severity
Medium (6.5)

Affected Version
5.9.3*

Visibility
Public

Status
Fixed

Found by

Piyush Patil
@xoffense
unranked

Fixed by

Jelmer Prins
@carakas
maintainer

This report was seen 333 times.

Jelmer Prins marked this as fixed with commit 76bf73 a year ago

Jelmer Prins has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

Chat with us