Cross-site Scripting (XSS) - Stored 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 "start_date" Parameter

🦹 Proof of Concept

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

Steps to reproduce issue

1- Login to Fork admin panel
2- Goto Modules=>Formbuilder
3- Turn on Burp Intercept
4- Click on "Update Filter"
5- Change value of "start_date" parameter to 22/03/2021'"()%26%25<yes>
<ScRiPt%20>alert(1)</ScRiPt>
6- Forward the request and XSS will be triggered
Video POC: https://drive.google.com/file/d/12PqUfuw3RFyOcFS0HIHfTkxrpsDDtACd/view?usp=sharing

💥 Impact

With the help of xss attacker can perform social engineering on users by redirecting them from real website to fake one. Attacker can steal their cookies leading to account takeover and download a malware on their system, and there are many more attacking scenarios a skilled attacker can perform with xss.

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

Severity
High (7.1)

High (7.1)

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 354 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