SQL Injection in forkcms/forkcms

Valid Reported on Oct 30th 2021

0

Description

When deleting submissions which belong to a formular (made with module `FormBuilder`), the parameter `id[]` is vulnerable for SQL injection.

Proof of Concept

Call the URL

```
http://127.0.0.1/private/en/form_builder/mass_data_action?form_id=2&token=a
```

To test this URL successfully, you need a valid formular and some submissions to that formular.
You might have to adjust the parameter `form_id` to another value.
After calling this URL, you have a new entry in `users` table.

Impact

The attacker can tamper data in the database as they want.

CVE
CVE-2022-0153
(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
Critical (9.6)

Visibility
Public

Status
Fixed

Found by

starkitsec
@starkitsec
unranked

Fixed by

Jelmer Prins
@carakas
maintainer

This report was seen 471 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 now considered stale. a year ago

Jelmer Prins has invalidated this vulnerability a year ago

csrf token fails and blocks this

The disclosure bounty has been dropped ✕

The fix bounty has been dropped ✕

Jelmer Prins a year ago

sorry, I was wrong, it is valid, I'll ask to reopen this one

Chat with us

Jamie Slome a year ago Admin

Jamie Slome a year ago Admin

Re-opened! ♥

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

fix is currently in review

Jelmer Prins marked this as fixed in 5.11.1 with commit 7a1204 8 months ago

Jelmer Prins has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation