

SQL injection through marking blog comments on bulk as spam in forkcms/forkcms



Valid

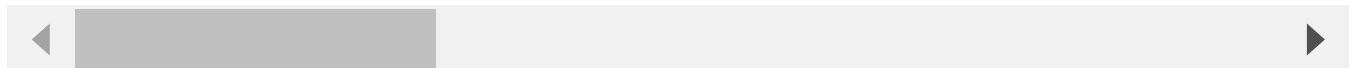
Reported on Mar 23rd 2022

Description

the comments ids aren't checked and vulnerable for SQL injection

Proof of Concept

`https://127.0.0.1:8001/private/en/blog/mass_comment_action?token=q58o77xs98`



Impact

This vulnerability is capable of injection sql

CVE

CVE-2022-1064

(Published)

Vulnerability Type

CWE-89: SQL Injection

Severity

Critical (9)

Visibility

Public

Status

Fixed

Found by



Jelmer Prins

@jprins

Chat with us



@carakas

maintainer

This report was seen 781 times.

We are processing your report and will contact the **forkcms** team within 24 hours. 8 months ago

Jelmer Prins modified the report 8 months ago

Jelmer Prins 8 months ago

Researcher

@admin found this one while writing fixes for other reported issues but it seems like I can't approve nor confirm it

Jamie Slome validated this vulnerability 8 months ago

Jelmer Prins has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Jamie Slome marked this as fixed in 5.11.1 with commit 6aca30 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

Chat with us

huntr

part of 418sec

main menu

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

partner menu

company

about

team

Chat with us