huntr

Cross-site Scripting (XSS) - Stored in orchardcms/orchardcore

0

✓ Valid Reported on Jan 11th 2022

Description

The application does not escape special characters before output to FE, lead to stored XSS.

Proof of Concept

Go to Workflows > Create Workflow > Add Task/Event
Set a title with XSS payload, e.g: `aa<svg/onload=alert('hacked')>`

Impact

XSS can have huge implications for a web application and its users. User accounts can be hijacked, change the html screen and insult the organization. Credentials could be stolen, sensitive data could be exfiltrated, and lastly, access to your client computers can be obtained.

CVE
CVE-2022-0243
(Published)

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

Severity
High (7.4)

Visibility
Public

Status
Fixed

Found by

laladee

@laladee

unranked

This report was seen 334 times.

We are processing your report and will contact the **orchardcms/orchardcore** team within 24 hours. 10 months ago

We have contacted a member of the **orchardcms/orchardcore** team and are waiting to hear back 10 months ago

We have sent a follow up to the **orchardcms/orchardcore** team. We will try again in 7 days. 10 months ago

A **orchardcms/orchardcore** maintainer validated this vulnerability 10 months ago

laladee has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **orchardcms/orchardcore** maintainer marked this as fixed in **1.2.2** with commit **218f25** 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us