huntr

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

0

✓ Valid Reported on Jan 6th 2022

Description

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

Proof of Concept

Example of a case:
Go to **Content > Content Types** `/Admin/ContentTypes/List`
Create or edit a type with XSS payload into `Display Name` field, e.g: `Social Meta Settings </title><svg/onload=alert('hacked')><title>`
Tick on the `Creatable` checkbox
Save and go to create new Type which edited above or go to Content > Content Items. Script will triggered

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.

Occurrences

Index.cshtml L54 ContentsAdminListCreate.cshtml L19 Hello.cshtml L25

CVE
CVE-2022-0159
(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 361 times.

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

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

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

A **orchardcms/orchardcore** maintainer validated this vulnerability a year 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 **1.2.1** with commit **4da927** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

ContentsAdminListCreate.cshtml#L19 has been validated ✓

Hello.cshtml#L25 has been validated ✓

Chat with us

Index.cshtml#L54 has been validated ✓

laladee 10 months ago

Researcher

@maintainer
your patch has not patched all locations. For example in the Workflows section, maybe I'll try to list them all in the next report

Sign in to join this conversation