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

0

Valid Reported on Jan 12th 2022

Description

The Stored XSS vulnerability occurs because the menu editing function can insert a JavaScript Scheme as the value of the menu's HREF.

Proof of Concept

```
1. Go to Content -> Menu -> Edit
2. Enter javascript:alert(document.domain) as the URL value using the Add c
3. After saving, use the Preview function to access and click the menu in t

Video : https://youtu.be/tAzuDCUhSZ4
```

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

Occurrences

C# AdminMenu.cs L3

I am sorry because I cannot found „ code„

CVE
CVE-2022-0274

(Published)

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

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

Pocas
@p0cas
amateur

This report was seen 367 times.

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

Pocas modified the report 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 10 months ago — Maintainer

I will evaluate the validity of the issue with other maintainers. This is not straightforward since the feature is supposed to let you be able to write custom HTML links on the front-end (this is a CMS). Outcomes could be to protect this feature behind a specific permission.

Pocas 10 months ago — Researcher

..? The vectors I found do not use HTML Injection. This occurs because the `ja` allowed when creating a simple link. In my experience, there seems to be no `javascript` scheme validation in this service.

A orchardcms/orchardcore maintainer 10 months ago Maintainer

I understand, and many web developers need to create menus that include javascript. This might explain why this input was not "sanitized". This is why I need to talk to other maintainers, to ensure it was not intentional.

Pocas 10 months ago Researcher

okay! I understood and I'll wait for your answer. Thank You

A orchardcms/orchardcore maintainer validated this vulnerability 10 months ago

Pocas 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 ✖

AdminMenu.cs#L3 has been validated ✔

Sign in to join this conversation