

Improper Authorization in orchardcms/orchardcore

0



Valid

Reported on Feb 24th 2022

Description

A low-privilege user (I tested it with `Editor` priv user) can create any `role` in the application.

Proof of Concept

Make a POST request to `/Admin/Roles/Create` using low-priv user's `cookie` and `__RequestVerificationToken`

A new role will be created with the specified name.

Impact

A low-priv user can create a number of roles which breaks the authorization principle of this application.

Occurrences

`C#` AdminController.cs L73-L123

CVE

CVE-2022-0821

(Published)

Vulnerability Type

CWE-285: Improper Authorization

Severity

High (7.1)

Visibility

Public

Status

Chat with us

Fixed

Found by



Rohan Sharma

@rohansh

unranked ▾

This report was seen 487 times.

We are processing your report and will contact the **orchardcms/orchardcore** team within 24 hours. 9 months ago

We have contacted a member of the **orchardcms/orchardcore** team and are waiting to hear back 9 months ago

We have sent a follow up to the **orchardcms/orchardcore** team. We will try again in 7 days. 9 months ago

A **orchardcms/orchardcore** maintainer validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

We have sent a fix follow up to the **orchardcms/orchardcore** team. We will try again in 7 days. 9 months ago

A **orchardcms/orchardcore** maintainer marked this as fixed in **1.3.0** with commit **b7096a** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

AdminController.cs#L73-L123 has been validated ✓

Sign in to join this conversation

Chat with us

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

[Chat with us](#)