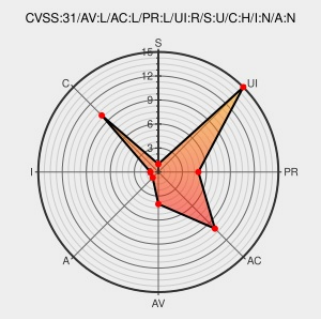
# CVE-2022-24742

Published on: Not Yet Published

Last Modified on: 06/30/2023 07:03:00 PM UTC

## **CVE-2022-24742** - advisory for GHSA-7563-75j9-6h5p

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Sylius from Sylius contain the following vulnerability:

Sylius is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, any other user can view the data if browser tab remains unclosed after log out. The issue is fixed in versions 1.9.10, 1.10.11, and 1.11.2. A workaround is available. The application must strictly redirect to login page even browser back button is pressed. Another possibility is to set more strict cache policies for restricted content.

CVE-2022-24742 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Sylius** - **Sylius** version **< 1.9.10**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.10.0, < 1.10.11**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.11.0, < 1.11.2**

### CVSS3 Score: 5.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | NONE | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Exposure of sensitive information by using the back button after logging out in sylius/sylius · Advisory · Sylius/Sylius · GitHub | github.com text/html | CONFIRM github.com/Sylius/Sylius/security/advisories/GHSA-7563-75j9-6h5p |
| Release v1.9.10 · Sylius/Sylius · GitHub | github.com text/html | MISC github.com/Sylius/Sylius/releases/tag/v1.9.10 |
| Release v1.10.11 · Sylius/Sylius · GitHub | github.com text/html | MISC github.com/Sylius/Sylius/releases/tag/v1.10.11 |
| Release v1.11.2 · Sylius/Sylius · GitHub | github.com text/html | MISC github.com/Sylius/Sylius/releases/tag/v1.11.2 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Sylius | Sylius | All | All | All | All |

cpe:2.3:a:sylius:sylius:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2022-24742 : Sylius is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, any ot… twitter.com/i/web/status/1… | 2022-03-14 19:24:20 |
| /r/netcve | CVE-2022-24742 | 2022-03-14 20:38:44 |

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status** status.cve.report