

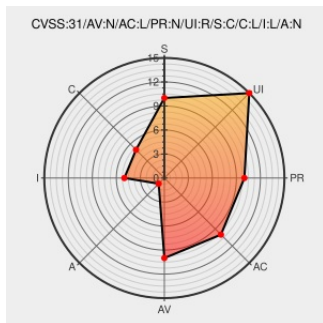


CVE-2022-24733

Published on: Not Yet Published

Last Modified on: 03/22/2022 05:32:00 PM UTC

CVE-2022-24733 - advisory for GHSA-4jp3-q2qm-9fmw

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Sylus](#) from [Sylus](#) contain the following vulnerability:

Sylus is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, it is possible for a page controlled by an attacker to load the website within an iframe. This will enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. The issue is

fixed in versions 1.9.10, 1.10.11, and 1.11.2. A workaround is available. Every response from app should have an X-Frame-Options header set to: ``sameorigin``. To achieve that, add a new `subscriber` in the app.

CVE-2022-24733 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Sylus](#) - **Sylus** version < 1.9.10

Affected Vendor/Software: [Sylus](#) - **Sylus** version >= 1.10.0, < 1.10.11

Affected Vendor/Software: [Sylus](#) - **Sylus** version >= 1.11.0, < 1.11.2

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality	Integrity	Availability

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description	Tags	Link
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
Add missing HTTP headers to avoid login forms clickjacking · Advisory · Sylius/Sylius · GitHub	github.com text/html	 CONFIRM github.com/Sylius/Sylius/security/advisories/GHSA-4jp3-q2qm-9fmw
Release v1.11.2 · Sylius/Sylius · GitHub	github.com text/html	 MISC github.com/Sylius/Sylius/releases/tag/v1.11.2

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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-2022-24733 : Sylius is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, it is... twitter.com/i/web/status/1...	2022-03-14 18:55:42
 /r/netcve	CVE-2022-24733	2022-03-14 19:38:22

← Previous ID

Next ID →

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)