

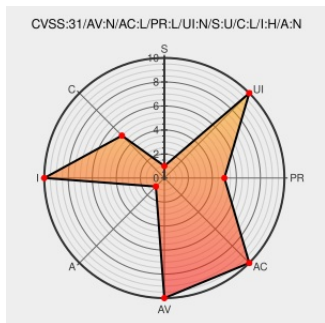


CVE-2022-24743

Published on: Not Yet Published

Last Modified on: 03/22/2022 03:06:00 PM UTC

CVE-2022-24743 - advisory for GHSA-mf3v-f2qq-pf9g

[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 1.10.11 and 1.11.2, the reset password token was not set to null after the password was changed. The same token could be used several times, which could result in leak of the existing token and unauthorized password change. The issue is fixed in versions 1.10.11 and 1.11.2. As

a workaround, overwrite the

`Sylus\Bundle\ApiBundle\CommandHandler\ResetPasswordHandler` class with code provided by the maintainers and register it in a container. More information about this workaround is available in the [GitHub Security Advisory](#).

CVE-2022-24743 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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

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

CVSS3 Score: **8.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	HIGH	NONE

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description	Tags	Link
Reset password token not set to null after reset password · Advisory · Sylius/Sylius · GitHub	github.com text/html	 CONFIRM github.com/Sylius/Sylius/security/advisories/GHSA-mf3v-f2qq-pf9g
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

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
<code>cpe:2.3:a:sylius:sylius:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-24743 : Sylius is an open source eCommerce platform. Prior to versions 1.10.11 and 1.11.2, the reset passw... twitter.com/i/web/status/1...	2022-03-14 21:07:36
 /r/netcve	CVE-2022-24743	2022-03-14 22:38:13

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)