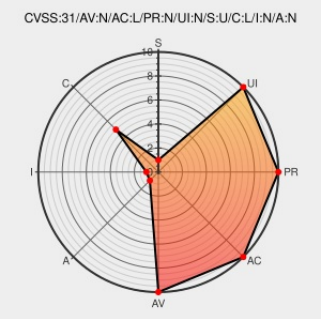
CVE-2021-32720

Published on: 06/28/2021 12:00:00 AM UTC

Last Modified on: 07/02/2021 04:51:00 PM UTC

CVE-2021-32720 - advisory for GHSA-rpxh-vg2x-526v

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 on top of Symfony. In versions of Sylius prior to 1.9.5 and 1.10.0-RC.1, part of the details (order ID, order number, items total, and token value) of all placed orders were exposed to unauthorized users. If exploited properly, a few additional information like the number of items in the cart and the date of the shipping may be fetched as well. This data seems to not be crucial nor is personal data, however, could be used for sociotechnical attacks or may expose a few details about shop condition to the third parties. The data possible to aggregate are the number of processed orders or their value in the moment of time. The problem has been patched at Sylius 1.9.5 and 1.10.0-RC.1. There are a few workarounds for the vulnerability. The first possible solution is to hide the problematic endpoints behind the firewall from not logged in users. This would put only the order list under the firewall and allow only authorized users to access it. Once a user is authorized, it will have access to theirs orders only. The second possible solution is to decorate the `\Sylius\Bundle\ApiBundle\Doctrine\QueryCollectionExtension\OrdersByLoggedInUserExtensio and throw `Symfony\Component\Security\Core\Exception\AccessDeniedException` if the class is executed for unauthorized user.

CVE-2021-32720 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.9.0, < 1.9.5**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.10.0-ALPHA.1, <= 1.10.0-BETA.1**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
List of order ids, number, items total and token value exposed for unauthorized uses via new API · Advisory · Sylius/Sylius · GitHub	github.com text/html	CONFIRM github.com/Sylius/Sylius/security/advisories/GHSA-rpxh-vg2x-526v
Release v1.9.5 · Sylius/Sylius · GitHub	github.com text/html	MISC github.com/Sylius/Sylius/releases/tag/v1.9.5

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-2021-32720 : Sylius is an Open Source eCommerce platform on top of Symfony. In versions of Sylius prior to 1.9.… twitter.com/i/web/status/1…	2021-06-28 18:48:45
/r/netcve	CVE-2021-32720	2021-06-28 19:41:13

← 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 registred 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