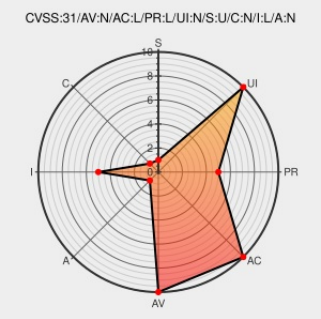
CVE-2020-15245

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:19:00 PM UTC

CVE-2020-15245 - advisory for GHSA-6gw4-x63h-5499

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



Certain versions of Sylius from Sylius contain the following vulnerability:

In Sylius before versions 1.6.9, 1.7.9 and 1.8.3, the user may register in a shop by email mail@example.com, verify it, change it to the mail another@domain.com and stay verified and enabled. This may lead to having accounts addressed to totally different emails, that were verified. Note, that this way one is not able to take over any existing account (guest or normal one). The issue has been patched in Sylius 1.6.9, 1.7.9 and 1.8.3. As a workaround, you may resolve this issue on your own by creating a custom event listener, which will listen to the sylius.customer.pre_update event. You can determine that email has been changed if customer email and user username are different. They are synchronized later on. Pay attention, to email changing behavior for administrators. You may need to skip this logic for them. In order to achieve this, you should either check master request path info, if it does not contain /admin prefix or adjust event triggered during customer update in the shop. You can find more information on how to customize the event here.

CVE-2020-15245 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 9.0.0, < 9.4.4**

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Ability to switch customer email address on account detail page and stay verified · Advisory · Sylius/Sylius · GitHub	Mitigation, Third Party Advisory, github.com, text/html	CONFIRM github.com/Sylius/Sylius/security/advisories/GHSA-6gw4-x63h-5499
[Shop] Disabling customer when email has been changed · Sylius/Sylius@60636d7 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/Sylius/Sylius/commit/60636d711a4011e8694d10d201b53632c7e8ecaf

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
Application	Sylius	Sylius	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

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