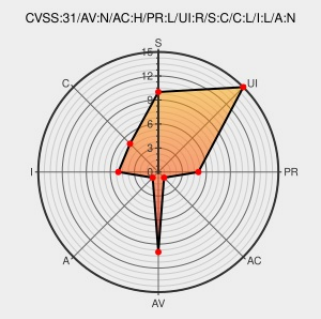
CVE-2020-5218

Published on: 01/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5218 - advisory for GHSA-prg5-hg25-8grq

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



Certain versions of Sylius from Sylius contain the following vulnerability:

Affected versions of Sylius give attackers the ability to switch channels via the _channel_code GET parameter in production environments. This was meant to be enabled only when kernel.debug is set to true. However, if no sylius_channel.debug is set explicitly in the configuration, the default value which is kernel.debug will be not resolved and cast to boolean, enabling this debug feature even if that parameter is set to false. Patch has been provided for Sylius 1.3.x and newer - 1.3.16, 1.4.12, 1.5.9, 1.6.5. Versions older than 1.3 are not covered by our security support anymore.

CVE-2020-5218 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Sylius** - **Sylius** version **< 1.3.13**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.4.0, < 1.4.6**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.5.0, < 1.5.1**

Affected Vendor/Software: **Sylius** - **Sylius** version **>= 1.6.0, < 1.6.3**

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	LOW	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication

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

CVE References

Description	Tags	Link
Ability to define unintended serialisation groups via HTTP header which might lead to data exposure · Advisory · Sylius/SyliusResourceBundle · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/Sylius/SyliusResourceBundle/security/advisories/GHSA-8vp7-j5cj-vvm2
security-advisories/CVE-2020-5220.yaml at master · FriendsOfPHP/security-advisories · GitHub	Third Party Advisory github.com text/html	MISC github.com/FriendsOfPHP/security-advisories/blob/master/sylius/resource-bundle/CVE-2020-5220.yaml

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	1.5.0	-	All	All
Application	Sylius	Sylius	All	All	All	All
Application	Sylius	Sylius	1.5.0	-	All	All

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

cpe:2.3:a:sylius:sylius:1.5.0:-:*:*:*:*:*:*:

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

cpe:2.3:a:sylius:sylius:1.5.0:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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