

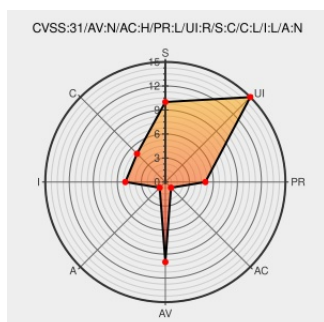


# CVE-2020-5218

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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |

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 | <div>Patch</div> <div>Third Party Advisory</div> <div>github.com</div> <div>text/html</div> | <div>CONFIRM</div> <div>github.com/Sylius/SyliusResourceBundle/security/advisories/GHSA-8vp7-j5cj-vvm2</div>                 |
| security-advisories/CVE-2020-5220.yaml at master · FriendsOfPHP/security-advisories · GitHub                                                          | <div>Third Party Advisory</div> <div>github.com</div> <div>text/html</div>                  | <div>MISC</div> <div>github.com/FriendsOfPHP/security-advisories/blob/master/sylius/resource-bundle/CVE-2020-5220.yaml</div> |

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](mailto: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      |
| 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, 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](#)