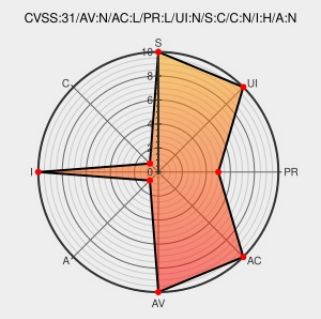
CVE-2020-15143

Published on: 08/19/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 06:33:00 PM UTC

CVE-2020-15143 - advisory for GHSA-p4pj-9g59-4ppv

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



Certain versions of Syliusresourcebundle from Sylius contain the following vulnerability:

In SyliusResourceBundle before versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4, rrequest parameters injected inside an expression evaluated by `symfony/expression-language` package haven't been sanitized properly. This allows the attacker to access any public service by manipulating that request parameter, allowing for Remote Code Execution. This issue has been patched for versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4. Versions prior to 1.3 were not patched.

CVE-2020-15143 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Sylius** - **SyliusResourceBundle** version **< 1.3.14**

Affected Vendor/Software: **Sylius** - **SyliusResourceBundle** version **>= 1.4.0 , < 1.4.7**

Affected Vendor/Software: **Sylius** - **SyliusResourceBundle** version **>= 1.5.0, < 1.5.2**

Affected Vendor/Software: **Sylius** - **SyliusResourceBundle** version **>= 1.6.0, < 1.6.4**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Remote Code Execution in ParametersParser while using request parameters inside expression language · Advisory · Sylius/SyliusResourceBundle · GitHub	Exploit Mitigation Third Party Advisory github.com text/html	CONFIRM github.com/Sylius/SyliusResourceBundle/security/advisories/GHSA-p4pj-9g59-4ppv

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sylius	Syliusresourcebundle	All	All	All	All
Application	Sylius	Syliusresourcebundle	All	All	All	All
Application	Sylius	Syliusresourcebundle	All	All	All	All
Application	Sylius	Syliusresourcebundle	All	All	All	All

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

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Symfony - CVE-2020-15143: github.com/Sylius/SyliusR…	2021-11-18 21:46:10

← Previous ID

Next ID→

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