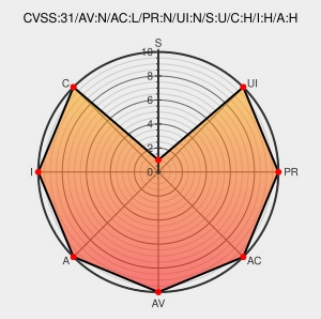
CVE-2022-24752

Published on: Not Yet Published

Last Modified on: 03/25/2022 12:42:00 PM UTC

CVE-2022-24752 - advisory for GHSA-2xmm-g482-4439

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



Certain versions of Syliusgridbundle from Sylius contain the following vulnerability:

SyliusGridBundle is a package of generic data grids for Symfony applications. Prior to versions 1.10.1 and 1.11-rc2, values added at the end of query sorting were passed directly to the database. The maintainers do not know if this could lead to direct SQL injections but took steps to remediate the vulnerability. The issue is fixed in versions 1.10.1 and 1.11-rc2. As a workaround, overwrite the`Sylius\Component\Grid\Sorting\Sorter.php` class and register it in the container. More information about this workaround is available in the GitHub Security Advisory.

CVE-2022-24752 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Sylius** - **SyliusGridBundle** version **< 1.10.1**

Affected Vendor/Software: **Sylius** - **SyliusGridBundle** version **1.11-alpha, <= 1.11-rc**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
DQL injection through sorting parameters blocked · Advisory · Sylius/SyliusGridBundle · GitHub	github.com text/html	CONFIRM github.com/Sylius/SyliusGridBundle/security/advisories/GHSA-2xmm-g482-4439
bug #222 [Security] Dql injection through sorting parameters blocked … · Sylius/SyliusGridBundle@73d0791 · GitHub	github.com text/html	MISC github.com/Sylius/SyliusGridBundle/commit/73d0791d0575f955e830a3da4c3345f420d2f7
[Security] Dql injection through sorting parameters blocked by lchrusciel · Pull Request #222 · Sylius/SyliusGridBundle · GitHub	github.com text/html	MISC github.com/Sylius/SyliusGridBundle/pull/222
Release v1.10.1 · Sylius/SyliusGridBundle · GitHub	github.com text/html	MISC github.com/Sylius/SyliusGridBundle/releases/tag/v1.10.1
Release v1.11.0-RC.2 · Sylius/SyliusGridBundle · GitHub	github.com text/html	MISC github.com/Sylius/SyliusGridBundle/releases/tag/v1.11.0-RC.2

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sylius	Syliusgridbundle	All	All	All	All
Application	Sylius	Syliusgridbundle	1.11.0	-	All	All
Application	Sylius	Syliusgridbundle	1.11.0	alpha1	All	All
Application	Sylius	Syliusgridbundle	1.11.0	beta1	All	All
Application	Sylius	Syliusgridbundle	1.11.0	rc1	All	All

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

cpe:2.3:a:sylius:syliusgridbundle:1.11.0:-:*:*:*:*:*:*:

cpe:2.3:a:sylius:syliusgridbundle:1.11.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:sylius:syliusgridbundle:1.11.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:sylius:syliusgridbundle:1.11.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24752 : SyliusGridBundle is a package of generic data grids for Symfony applications. Prior to versions 1.… twitter.com/i/web/status/1…	2022-03-15 14:44:43
/r/netcve	CVE-2022-24752	2022-03-15 15:38:42

← Previous ID

Next ID→