



CVE-2022-24749

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-24749
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-14 22:15:00 UTC
Updated	2022-03-22 15:08:00 UTC
Description	Sylius is an open source eCommerce platform. In versions prior to 1.9.10, 1.10.11, and 1.11.2, it is possible to upload an S

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	L
Release v1.9.10 · Sylius/Sylius · GitHub	MISC	g
Improper sanitize of SVG files during content upload ('Cross-site Scripting') in Sylius/Sylius · Advisory · Sylius/Sylius · GitHub	CONFIRM	g
Release v1.10.11 · Sylius/Sylius · GitHub	MISC	g
Release v1.11.2 · Sylius/Sylius · GitHub	MISC	g
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API cve.report/api

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