



CVE-2020-26223

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

Summary

CVE	CVE-2020-26223
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-13 18:15:00 UTC
Updated	2020-11-30 16:18:00 UTC
Description	Spree is a complete open source e-commerce solution built with Ruby on Rails. In Spree from version 3.7 and before versio

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spreecommerce	Spree	All	All	All	All
Application	Spreecommerce	Spree	All	All	All	All

References

Reference	Source
Storefront API v2 Spree Commerce Documentation	MISC
Fix security issue in order status endpoint by kshalot · Pull Request #10573 · spree/spree · GitHub	MISC
Passing an empty string " as the token allows to query any complete order without knowing it's token · Advisory · spree/spree · GitHub	CONFIRMED
CVE Program record	CVE
NVD vulnerability detail	NVD

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