



CVE-2020-15269

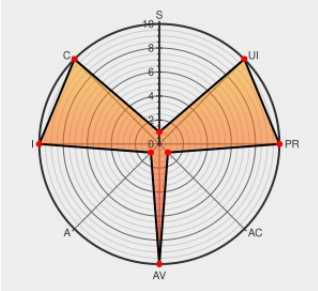
Published on: 10/20/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:21:00 PM UTC

CVE-2020-15269 - advisory for GHSA-f8cm-364f-q9qh

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Spree](#) from [Sparksolutions](#) contain the following vulnerability:

In Spree before versions 3.7.11, 4.0.4, or 4.1.11, expired user tokens could be used to access Storefront API v2 endpoints. The issue is patched in versions 3.7.11, 4.0.4 and 4.1.11. A workaround without upgrading is described in the linked advisory.

CVE-2020-15269 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: spree - spree version < 3.7.11

Affected Vendor/Software: spree - spree version >= 4.0.0, < 4.0.4

Affected Vendor/Software: spree - spree version >= 4.1.0, < 4.1.11

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description

ensure doorkeeper_token is valid when authenticating requests in v2 · spree/spree@e43643a · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

MISC

github.com/spree/spree/commit/e43643abfe51f54bd9208dd02298b366e9b9a847

Description

Ensure that doorkeeper_token is valid when authenticating requests in API v2 calls · Advisory · spree/spree · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/spree/spree/security/advisories/GHSA-f8cm-364f-q9qh

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sparksolutions	Spree	All	All	All	All
Application	Sparksolutions	Spree	All	All	All	All
cpe:2.3:a:sparksolutions:spree:*.***.***.***:						
cpe:2.3:a:sparksolutions:spree:*.***.***.***:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →