



CVE-2020-13674

Published on: 02/11/2022 12:00:00 AM UTC

Last Modified on: 02/18/2022 01:42:00 AM UTC

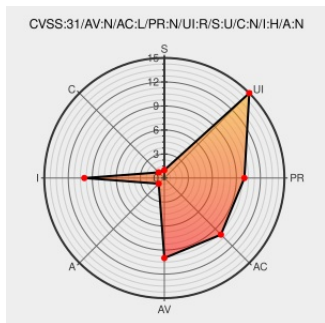
CVE-2020-13674

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The QuickEdit module does not properly validate access to routes, which could allow cross-site request forgery under some circumstances and lead to possible data integrity issues. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. Removing the "access in-place editing" permission from untrusted users will not fully mitigate the vulnerability.

CVE-2020-13674 has been assigned by [security@drupal.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Drupal](#) - Core version < 9.2.6

Affected Vendor/Software: [Drupal](#) - Core version < 9.1.13

Affected Vendor/Software: [Drupal](#) - Core version < 8.9.19

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description

Tags

Link

Drupal core - Moderately critical - Cross Site Request Forgery - SA-CORE-2021-007 | Drupal.org

web.archive.org

text/html

Inactive Link

Not Archived

CONFIRM

www.drupal.org/sa-core-2021-007

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.

Related QID Numbers

730199

Drupal Core Multiple Vulnerabilities (SA-CORE-2021-006 - SA-CORE-2021-010)

730201

Drupal Core Cross-Site Request Forgery (CSRF) Vulnerability (SA-CORE-2021-007)

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application

Drupal

Drupal

All

All

All

All

cpe:2.3:a:drupal:drupal.*.*.*.*.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

Social Mentions

Source

Title

Posted (UTC)

🔍

@CVEreport

CVE-2020-13674 : The QuickEdit module does not properly validate access to routes, which could allow cross-site req... [twitter.com/i/web/status/1...](https://twitter.com/i/web/status/1222222222)

2022-02-11 15:53:02

🔍

@WesUncensored

New vulnerability on the NVD: CVE-2020-13674 ift.tt/stKXOf

2022-02-11 17:34:11

🔍

/r/netcve

[CVE-2020-13674](#)

2022-02-11 16:38:37

← Previous ID

Next ID →