



CVE-2020-13675

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

Summary

CVE	CVE-2020-13675
State	PUBLIC
Assigner	security@drupal.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-11 16:15:00 UTC
Updated	2022-02-18 01:44:00 UTC
Description	Drupal's JSON:API and REST/File modules allow file uploads through their HTTP APIs. The modules do not correctly run a

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Drupal core - Moderately critical - Access bypass - SA-CORE-2021-008 Drupal.org	CONFIRM	www.drupal.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730199](#) Drupal Core Multiple Vulnerabilities (SA-CORE-2021-006 - SA-CORE-2021-010)

[730202](#) Drupal Core Access Bypass Vulnerability (SA-CORE-2021-008)

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