CVE-2019-6340

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-6340
State	PUBLIC
Assigner	security@drupal.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-21 21:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6.x before

Risk And Classification

EPSS: 0.944360000 probability, percentile 0.999870000 (date 2026-05-08)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Drupal
Product	Core
Name	Drupal Core Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-6340

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Drupal < 8.6.9 - REST Module Remote Code Execution - PHP webapps Exploit	EXPLOIT-
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution - PHP webapps Exploit	EXPLOIT-
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit) - PHP remote Exploit	EXPLOIT-

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003 | Drupal.org	CONFIRM
Synology Inc.	CONFIRM
Drupal Core CVE-2019-6340 Arbitrary PHP Code Execution Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

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