

CVE-2019-6340

Drupal Core Remote Code Execution Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

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 8.6.10. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this if one of the following conditions is met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7.

EVRS 83_{/100} Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.920 99.82nd percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.920 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

(Note: The Drupal 7 Services module itself does not require an update at this time, but you should apply other contributed updates associated with this advisory if Services is in use.)

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
drupal/core	≥ 8.6.0, < 8.6.10	8.6.10	GitHub
drupal/core	≥ 7.0.0, < 7.62.0	7.62.0	GitHub
drupal/core	≥ 8.0.0, < 8.5.11	8.5.11	GitHub
drupal/drupal	≥ 7.0.0, < 7.62.0	7.62.0	GitHub
drupal/drupal	≥ 8.0.0, < 8.5.11	8.5.11	GitHub
drupal/drupal	≥ 8.6.0, < 8.6.10	8.6.10	GitHub
drupal	≥ 8.5.0 < 8.5.11 ≥ 8.6.0 < 8.6.10	8.5.11 · 8.6.10	NVD

Sources

Vendor guidance exploit-db.com/exploits/46452/
NVD nvd.nist.gov/vuln/detail/CVE-2019-6340

Additional guidance drupal.org/sa-core-2019-003
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

GitHub advisory github.com/advisories/GHSA-3gx6-h57h-rm27

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-2184

Current data evulnable.com/vulnerability-management/cve/CVE-2019-6340

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.