

CVE-2018-7600

Drupal Core Remote Code Execution Vulnerability

Exigent
CISA KEV since Nov 3, 2021
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
drupal/core	≥ 7.0, < 7.58	7.58	GitHub
drupal/core	≥ 8.0, < 8.3.9	8.3.9	GitHub
drupal/core	≥ 8.4.0, < 8.4.6	8.4.6	GitHub
drupal/core	≥ 8.5.0, < 8.5.1	8.5.1	GitHub
drupal/drupal	≥ 7.0, < 7.58	7.58	GitHub
drupal/drupal	≥ 8.0, < 8.3.9	8.3.9	GitHub
drupal/drupal	≥ 8.4, < 8.4.6	8.4.6	GitHub
drupal/drupal	≥ 8.5, < 8.5.1	8.5.1	GitHub
drupal	≤ 7.57 ≥ 8.0.0 < 8.3.9 ≥ 8.4.0 < 8.4.6 ≥ 8.5.0 < 8.5.1	no fixed version listed	NVD
debian linux	7.0 8.0 9.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/g0rx/CVE-2018-7600-Drupal-RCE
NVD nvd.nist.gov/vuln/detail/CVE-2018-7600

GitHub advisory github.com/advisories/GHSA-7fh9-933g-885p

Current data evulnable.com/vulnerability-management/cve/CVE-2018-7600

Additional guidance groups.drupal.org/security/faq-2018-002
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-2985

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