

CVE-2022-26352

dotCMS Unrestricted Upload of File Vulnerability

Exigent
CISA KEV since Aug 25, 2022
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

An issue was discovered in the ContentResource API in dotCMS 3.0 through 22.02. Attackers can craft a multipart form request to post a file whose filename is not initially sanitized. This allows directory traversal, in which the file is saved outside of the intended storage location. If anonymous content creation is enabled, this allows an unauthenticated attacker to upload an executable file, such as a .jsp file, that can lead to remote code execution.

EVRS 91 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.912 99.81st percentile · FIRST	CISA DEADLINE Sep 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.912 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
dotcms	≥ 3.0 ≤ 22.02	after 22.02	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-pr6q-gfg3-vcjf	dotcms.com	dotcms.com/security/SI-62
NVD	nvd.nist.gov/vuln/detail/CVE-2022-26352	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-30911	Current data	evulnable.com/vulnerability-management/cve/CVE-2022-26352

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