

CVE-2017-9822

DotNetNuke (DNN) Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

DNN (aka DotNetNuke) before 9.1.1 has Remote Code Execution via a cookie, aka "2017-08 (Critical) Possible remote code execution on DNN sites."

EVRS 91 /100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.948 99.86th 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	0.948 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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
DotNetNuke.Core	< 9.1.1	9.1.1	GitHub
dotnetnuke	< 9.1.1	9.1.1	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2017-9822

GitHub advisory github.com/advisories/GHSA-x2rg-fmfv-crq5

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-0710

Current data evulnable.com/vulnerability-management/cve/CVE-2017-9822

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