CVE-2018-15811

DotNetNuke (DNN) Inadequate Encryption Strength Vulnerability

CISA KEV since Nov 3, 2021 | Actively exploited | Public exploit module (Metasploit)

DNN (aka DotNetNuke) 9.2 through 9.2.1 uses a weak encryption algorithm to protect input parameters.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
78/100	7.5	0.763	May 3, 2022
Urgent priority	High · NVD	99.54th percentile · FIRST	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**	No known ransomware campaign association	⊟ **KEV recency**	On the CISA KEV catalog for over two years
☑ **EPSS**	0.763 probability	⊟ **Pre-patch disclosure**	Disclosure status unavailable
☑ **CVSS**	Base score 7.5	⊟ **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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
DotNetNuke.Core	⩾ 9.2.0, < 9.2.2	9.2.2	GitHub
dotnetnuke	⩾ 9.2 ⩽ 9.2.1	after 9.2.1	NVD

Sources

Vendor guidance	dnnsoftware.com/community/security/security-center	**NVD**	nvd.nist.gov/vuln/detail/CVE-2018-15811
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	**GitHub advisory**	github.com/advisories/GHSA-h595-8pw6-5q6v
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-0590	**Current data**	evulnable.com/vulnerability-management/cve/CVE-2018-15811

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