CVE-2018-18325

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-18325
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-03 17:15:00 UTC
Updated	2023-03-03 20:46:00 UTC
Description	DNN (aka DotNetNuke) 9.2 through 9.2.2 uses a weak encryption algorithm to protect input parameters. NOTE: this issue e

Risk And Classification

EPSS: 0.929600000 probability, percentile 0.997790000 (date 2026-04-17)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-326

CISA Known Exploited Vulnerability

Vendor	DotNetNuke (DNN)
Product	DotNetNuke (DNN)
Name	DotNetNuke (DNN) Inadequate Encryption Strength Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-18325

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dnnsoftware	Dotnetnuke	All	All	All	All

References

Reference	Source	Link	Tags
DotNetNuke Cookie Deserialization Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
Releases · dnnsoftware/Dnn.Platform · GitHub	MISC	github.com	Release Notes, Third
DNN Security Updates | DNN (DotNetNuke)	MISC	www.dnnsoftware.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730389 DNN (DotNetNuke) Weak Encryption Algorithm Vulnerability

981691 Dotnet (nuget) Security Update for DotNetNuke.Core (GHSA-j3g9-6fx5-gjv7)