



# CVE-2018-18325

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-18325
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-03 17:15:00 UTC
<b>Updated</b>	2023-03-03 20:46:00 UTC
<b>Description</b>	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

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	All	All	All	All

## References

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

NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	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)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)