CVE-2020-5187

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

Summary

CVE	CVE-2020-5187
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-24 15:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	DNN (formerly DotNetNuke) through 9.4.4 allows Path Traversal (issue 2 of 2).

Risk And Classification

Problem Types: CWE-22

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 CMS 9.4.4 Zip Directory Traversal ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Pa
DNN (DotNetNuke) CMS, not as secure as you think | by Sajjad Pourali | Medium	MISC	medium.com	Third Party Advis
Releases · dnnsoftware/Dnn.Platform · GitHub	MISC	github.com	Release Notes,
DNN (DotNetNuke) CMS, not as secure as you think | by Sajjad Pourali | Medium		medium.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report