



CVE-2013-4649

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-4649
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-12 14:55:30 UTC
Updated	2026-04-24 17:34:37 UTC
Description	Cross-site scripting (XSS) vulnerability in DotNetNuke (DNN) before 6.2.9 and 7.x before 7.1.1 allows remote attackers to ir

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS: 0.002690000 probability, percentile 0.503940000 (date 2026-04-26)

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Dnnsoftware	Dotnetnuke	1.0.10d	All	All	All
Application	Dnnsoftware	Dotnetnuke	1.0.10e	All	All	All
Application	Dnnsoftware	Dotnetnuke	1.0.6	All	All	All
Application	Dnnsoftware	Dotnetnuke	1.0.7	All	All	All
Application	Dnnsoftware	Dotnetnuke	1.0.8	All	All	All
Application	Dnnsoftware	Dotnetnuke	1.0.9	All	All	All
Application	Dnnsoftware	Dotnetnuke	2.1.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	2.1.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	3.0.11	All	All	All
Application	Dnnsoftware	Dotnetnuke	3.0.7	All	All	All
Application	Dnnsoftware	Dotnetnuke	3.0.8	All	All	All
Application	Dnnsoftware	Dotnetnuke	3.1.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	3.3.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.3.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.4.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.5.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.5.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.5.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.6.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.6.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.6.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.7.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.8.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.8.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.8.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.8.3	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.8.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.9	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.9.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.9.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.05.01	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.06.00	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.1.1	All	All	All

Application	Dnnsoftware	Dotnetnuke	5.1.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.1.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.1.3	All	All	All
Application	Dnnsoftware	Dotnetnuke	5.1.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.0.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.0.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.0.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.3	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.1.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.3	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.6	All	All	All
Application	Dnnsoftware	Dotnetnuke	6.2.7	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.2	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.3	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.4	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.5	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.0.6	All	All	All
Application	Dnnsoftware	Dotnetnuke	7.1.0	All	All	All
Application	Dnnsoftware	Dotnetnuke	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	

References						
Reference	Source			Link		

DotNetNuke (DNN) 7.1.0 / 6.2.8 Cross Site Scripting ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packetstormsecurity.com
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108	secunia.com
DNN Security Updates DNN CMS & Online Community Platform	af854a3a-2127-422b-91ae-364da2661108	www.dnnsoftware.com
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



No vendor comments have been submitted for this CVE.

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