



CVE-2005-0040

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

Summary

CVE	CVE-2005-0040
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-19 04:00:00 UTC
Updated	2026-04-24 17:34:37 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in DotNetNuke before 3.0.12 allow remote attackers to inject arbitrary web

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: 0.005270000 probability, percentile 0.671760000 (date 2026-04-26)

Problem Types: NVD-CWE-Other | 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	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		
404 Not Found			af854a3a-2127-422b-91ae-364da2661108	www.woan		
DotNetNuke User-Agent String Application Logs HTML Injection Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securi		
Secunia - Advisories - DotNetNuke Script Insertion Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108	secunia.co		
DotNetNuke User Registration Information HTML Injection Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securi		
DotNetNuke Failed Logon Username Application Logs HTML Injection Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securi		
'DotNetNuke (Multiple XSS)' - MARC			af854a3a-2127-422b-91ae-364da2661108	marc.info		
CVE Program record			CVE.ORG	www.cve.o		
NVD vulnerability detail			NVD	nvd.nist.go		
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						