



# CVE-2006-4973

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

## Summary

<b>CVE</b>	CVE-2006-4973
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-09-25 01:07:00 UTC
<b>Updated</b>	2026-04-24 17:34:37 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in Default.aspx in Perpetual Motion Interactive Systems DotNetNuke before 3.3.5, a

## 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:** 0.010820000 probability, percentile 0.779310000 (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	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.10d	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.10e	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.6	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.7	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.8	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	1.0.9	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	2.1.1	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	2.1.2	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	3.0.7	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	3.0.8	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	3.1.0	All	All	All
Application	<a href="#">Dnnsoftware</a>	<a href="#">Dotnetnuke</a>	4.0	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
Security Bulletin no.3	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.d...</a>
Security Advisory - VULN20-09-2006	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.se...</a>
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	<a href="#">exchan...</a>
DotNetNuke HTML Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.se...</a>
DotNetNuke "error" Parameter Cross-Site Scripting Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	<a href="#">secunia...</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.v...</a>
CVE Program record	CVE.ORG	<a href="#">www.cv...</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis...</a>

No vendor comments have been submitted for this CVE.

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

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). 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)