



CVE-2012-1036

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2012-1036
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-11 10:39:26 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the telerik HTML editor in DotNetNuke before 5.6.4 and 6.x before 6.1.0 allows re

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: 0.002630000 probability, percentile 0.496710000 (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	4.9.1	All	All	All
Application	Dnnsoftware	Dotnetnuke	4.9.2	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	All	All	All	All
Application	Dotnetnuke	Dotnetnuke	4.9.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	4.9.3	All	All	All
Application	Dotnetnuke	Dotnetnuke	4.9.4	All	All	All
Application	Dotnetnuke	Dotnetnuke	4.9.5	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.0.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.0.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.1.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.2.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.2.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.2.2	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.2.3	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.3.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.3.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.4.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.4.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.4.2	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.4.3	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.4.4	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.5.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.5.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.6.0	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.6.1	All	All	All
Application	Dotnetnuke	Dotnetnuke	5.6.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	Na	N/a	affected n/a	Not specified
-----	----	-----	--------------	---------------

References

Reference	Source
Microsoft Vulnerability Research Advisory MSVR12-002: Vulnerability in DotNetNuke Could Allow Arbitrary Script Execution	af854a3a-2127
Security bulletin no.59	af854a3a-2127
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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

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