



# Access bypass in Drupal 7 i18n\_node translation UI

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

## Summary

<b>CVE</b>	CVE-2026-0748
<b>State</b>	PUBLISHED
<b>Assigner</b>	drupal
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 22:16:27 UTC
<b>Updated</b>	2026-04-01 16:22:14 UTC
<b>Description</b>	In the Drupal 7 Internationalization (i18n) module, the i18n_node submodule allows a user with both "Translate content" and

## Risk And Classification

**Primary CVSS:** v4.0 5.3 MEDIUM from mlhess@drupal.org

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000330000 probability, percentile 0.095990000 (date 2026-04-01)

**Problem Types:** CWE-284 | CWE-276 | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
4.0	mlhess@drupal.org	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N
3.1	nvd@nist.gov	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Internationalization Project	Internationalization	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Drupal	Internationalization I18n - I18n Node Submodule	affected 7.x-1.0 7.x-1.35 custom	Not specified

## References

Reference	Source	Link	Tags
<a href="http://www.herodevs.com/vulnerability-directory/cve-2026-0748">www.herodevs.com/vulnerability-directory/cve-2026-0748</a>	<a href="mailto:mlhess@drupal.org">mlhess@drupal.org</a>	<a href="http://www.herodevs.com">www.herodevs.com</a>	Exploit, Third P
<a href="http://www.herodevs.com/vulnerability-directory/cve-2026-0748">www.herodevs.com/vulnerability-directory/cve-2026-0748</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="http://www.herodevs.com">www.herodevs.com</a>	Exploit, Third P
<a href="http://d7es.tag1.com/node/86">d7es.tag1.com/node/86</a>	<a href="mailto:mlhess@drupal.org">mlhess@drupal.org</a>	<a href="http://d7es.tag1.com">d7es.tag1.com</a>	Third Party Adv
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

## Vendor Comments And Credit

### Discovery Credit

**CNA:** [Tatár Balázs János \(tatarbj\)](#) (en)

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)