



CVE-2015-2821

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-2821
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-01 14:59:00 UTC
Updated	2016-12-03 03:06:00 UTC
Description	TYPO3 Neos 1.1.x before 1.1.3 and 1.2.x before 1.2.3 allows remote editors to access, create, and modify content nodes in

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Neos	1.1.0	All	All	All
Application	Typo3	Neos	1.1.1	All	All	All
Application	Typo3	Neos	1.1.2	All	All	All
Application	Typo3	Neos	1.2.0	All	All	All
Application	Typo3	Neos	1.2.1	All	All	All
Application	Typo3	Neos	1.2.2	All	All	All
Application	Typo3	Neos	1.1.0	All	All	All
Application	Typo3	Neos	1.1.1	All	All	All
Application	Typo3	Neos	1.1.2	All	All	All
Application	Typo3	Neos	1.2.0	All	All	All
Application	Typo3	Neos	1.2.1	All	All	All
Application	Typo3	Neos	1.2.2	All	All	All

References

Reference	Source	Link	Tags
TYPO3 Neos Extension CVE-2015-2821 Remote Privilege Escalation Vulnerability	BID	www.securityfocus.com	
TYPO3-NEOS-SA-2015-001: Privilege Escalation in TYPO3 Neos	CONFIRM	typo3.org	Patch, Vendor Ac

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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