CVE-2014-6231

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-6231
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-11 14:16:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Unspecified vulnerability in the CWT Frontend Edit (cwt_feedit) extension before 1.2.5 for TYPO3 allows remote authentica

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cwt Frontend Edit Project	Cwt Frontend Edit	All	All	All	All

References

Reference	Source
Several vulnerabilities in third party extensions - - TYPO3 - The Enterprise Open Source CMS	MISC
CWT Frontend Edit (cwt_feedit) - - TYPO3 - The Enterprise Open Source CMS	CONFIRM
IBM X-Force Exchange	XF
TYPO3 CWT Frontend Edit Extension Unspecified Remote Code Execution Vulnerability	BID
Security Advisory SA60888 - TYPO3 CWT Frontend Edit Extension Unspecified Arbitrary Code Execution Vulnerability - Secunia	SECUNIA
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 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 registred 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

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