CVE-2015-8755

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

Summary

CVE	CVE-2015-8755
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-08 19:59:21 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in unspecified backend components in TYPO3 6.2.x before 6.2.16 and 7.x

Risk And Classification

Primary CVSS: v3.0 5.4 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Problem Types: CWE-79 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	3.5		AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:S/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	6.2.0	All	All	All
Application	Typo3	Typo3	6.2.0	alpha1	All	All
Application	Typo3	Typo3	6.2.0	alpha2	All	All
Application	Typo3	Typo3	6.2.0	alpha3	All	All
Application	Typo3	Typo3	6.2.0	beta1	All	All
Application	Typo3	Typo3	6.2.0	beta2	All	All
Application	Typo3	Typo3	6.2.0	beta3	All	All
Application	Typo3	Typo3	6.2.0	beta4	All	All
Application	Typo3	Typo3	6.2.0	beta5	All	All
Application	Typo3	Typo3	6.2.0	beta6	All	All
Application	Typo3	Typo3	6.2.0	beta7	All	All
Application	Typo3	Typo3	6.2.0	rc1	All	All
Application	Typo3	Typo3	6.2.0	rc2	All	All
Application	Typo3	Typo3	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.10	All	All	All
Application	Typo3	Typo3	6.2.10	rc1	All	All
Application	Typo3	Typo3	6.2.11	All	All	All

Application	Typo3	Typo3	6.2.12	All	All	All
Application	Typo3	Typo3	6.2.13	All	All	All
Application	Typo3	Typo3	6.2.14	All	All	All
Application	Typo3	Typo3	6.2.15	All	All	All
Application	Typo3	Typo3	6.2.2	All	All	All
Application	Typo3	Typo3	6.2.3	All	All	All
Application	Typo3	Typo3	6.2.4	All	All	All
Application	Typo3	Typo3	6.2.5	All	All	All
Application	Typo3	Typo3	6.2.6	All	All	All
Application	Typo3	Typo3	6.2.7	All	All	All
Application	Typo3	Typo3	6.2.8	All	All	All
Application	Typo3	Typo3	6.2.9	All	All	All
Application	Typo3	Typo3	7.0.0	All	All	All
Application	Typo3	Typo3	7.0.2	All	All	All
Application	Typo3	Typo3	7.1.0	All	All	All
Application	Typo3	Typo3	7.2.0	All	All	All
Application	Typo3	Typo3	7.3.0	All	All	All
Application	Typo3	Typo3	7.3.1	All	All	All
Application	Typo3	Typo3	7.4.0	All	All	All
Application	Typo3	Typo3	7.5.0	All	All	All
Application	Typo3	Typo3	7.6.0	All	All	All
Application	Typo3	Typo3	7.6.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
TYPO3 Input Validation Flaw in Backend Components Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	af854a3a-2127-
Multiple Cross-Site Scripting vulnerabilities in TYPO3 backend - - TYPO3 - The Enterprise Open Source CMS	af854a3a-2127-
TYPO3 Backend Components Multiple Cross Site Scripting Vulnerabilities	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.

Free CVE JSON API cve.report/api

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