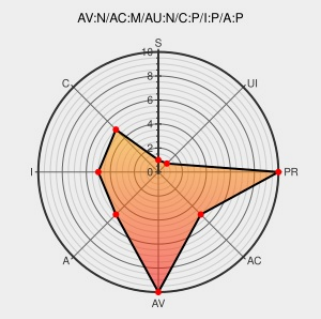
CVE-2011-4614

Published on: 02/17/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

CVE-2011-4614

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Typo3 from Typo3 contain the following vulnerability:

PHP remote file inclusion vulnerability in Classes/Controller/AbstractController.php in the workspaces system extension in TYPO3 4.5.x before 4.5.9, 4.6.x before 4.6.2, and development versions of 4.7 allows remote attackers to execute arbitrary PHP code via a URL in the BACK_PATH parameter.

CVE-2011-4614 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
TYPO3 - the Enterprise Open Source CMS: TYPO3 Security Bulletin TYPO3-CORE-SA-2010-004: Critical Vulnerability in TYPO3 Core	Patch, Vendor Advisory, typo3.org, text/html	CONFIRM typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2011-004/
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 77776
Page Not Found	typo3.org, text/x-diff, Inactive Link, Not Archived	CONFIRM typo3.org/fileadmin/security-team/bug32571/32571.diff
Security Alerts - Secunia	Vendor Advisory, web.archive.org	SECUNIA 47201

	text/html	
oss-security - TYPO3 typo3-core-sa-2011-004	www.openwall.com text/html	MLIST [oss-security] 20111216 TYPO3 typo3-core-sa-2011-004

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	4.5	All	All	All
Application	Typo3	Typo3	4.5.1	All	All	All
Application	Typo3	Typo3	4.5.2	All	All	All
Application	Typo3	Typo3	4.5.3	All	All	All
Application	Typo3	Typo3	4.5.4	All	All	All
Application	Typo3	Typo3	4.5.5	All	All	All
Application	Typo3	Typo3	4.5.6	All	All	All
Application	Typo3	Typo3	4.5.7	All	All	All
Application	Typo3	Typo3	4.5.8	All	All	All
Application	Typo3	Typo3	4.6	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All
Application	Typo3	Typo3	4.5	All	All	All
Application	Typo3	Typo3	4.5.1	All	All	All
Application	Typo3	Typo3	4.5.2	All	All	All
Application	Typo3	Typo3	4.5.3	All	All	All
Application	Typo3	Typo3	4.5.4	All	All	All
Application	Typo3	Typo3	4.5.5	All	All	All
Application	Typo3	Typo3	4.5.6	All	All	All
Application	Typo3	Typo3	4.5.7	All	All	All
Application	Typo3	Typo3	4.5.8	All	All	All
Application	Typo3	Typo3	4.6	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All

cpe:2.3:a:typo3:typo3:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.6.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→