



CVE-2010-5099

Published on: 05/30/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:06 PM UTC

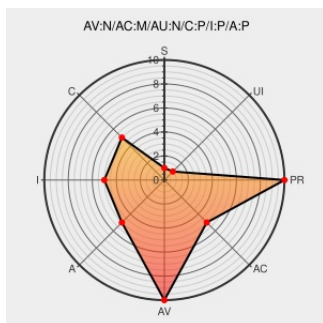
CVE-2010-5099

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Typo3](#) from [Typo3](#) contain the following vulnerability:

The fileDenyPattern functionality in the PHP file inclusion protection API in TYPO3 4.2.x before 4.2.16, 4.3.x before 4.3.9, and 4.4.x before 4.4.5 does not properly filter file types, which allows remote attackers to bypass intended access restrictions and access arbitrary PHP files, as demonstrated using path traversal sequences with %00 null bytes and CVE-2010-3714 to read the TYPO3 encryption key from localconf.php.

CVE-2010-5099 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

TYPO3 Unauthenticated Arbitrary File Retrieval

[Exploit](#)
www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 15856](#)

TYPO3 Multiple Vulnerabilities - Advisories - Community

[Vendor Advisory](#)
web.archive.org
[text/html](#)

[SECUNIA 35770](#)

oss-security - CVE requests: ftpls, xdigger, lbreakout2, calibre, typo3

www.openwall.com
[text/html](#)

[MLIST \[oss-security\] 20110113](#)
CVE requests: ftpls, xdigger,
lbreakout2, calibre, typo3

oss-security - CVE-request: TYPO3 TYPO3-SA-2010-022 still

www.openwall.com

[MI IST \[oss-security\] 20120511](#)

oss-security - CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE	www.openwall.com text/html	MLIST [oss-security] 20120511 CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE
Nibble Security: TYPO3-SA-2010-020, TYPO3-SA-2010-022 explained	blog.nibblesec.org text/html	MISC blog.nibblesec.org/2010/12/typo3-sa-2010-020-typo3-sa-2010-022.html
TYPO3 - the Enterprise Open Source CMS: TYPO3 Security Bulletin TYPO3-SA-2010-022: Multiple vulnerabilities in TYPO3 Core	typo3.org text/html	CONFIRM typo3.org/teams/security/security-bulletins/typo3-core/typo3-sa-2010-022/">typo3.org/teams/security/security-bulletins/typo3-core/typo3-sa-2010-022/
oss-security - Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE	www.openwall.com text/html	MLIST [oss-security] 20120512 Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE
oss-security - Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE	www.openwall.com text/html	MLIST [oss-security] 20120510 Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF typo3-unspecified-file-include(64180)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	4.2.0	All	All	All
Application	Typo3	Typo3	4.2.1	All	All	All
Application	Typo3	Typo3	4.2.10	All	All	All
Application	Typo3	Typo3	4.2.11	All	All	All
Application	Typo3	Typo3	4.2.12	All	All	All
Application	Typo3	Typo3	4.2.13	All	All	All
Application	Typo3	Typo3	4.2.14	All	All	All
Application	Typo3	Typo3	4.2.15	All	All	All
Application	Typo3	Typo3	4.2.2	All	All	All
Application	Typo3	Typo3	4.2.3	All	All	All
Application	Typo3	Typo3	4.2.4	All	All	All
Application	Typo3	Typo3	4.2.5	All	All	All
Application	Typo3	Typo3	4.2.6	All	All	All
Application	Typo3	Typo3	4.2.7	All	All	All
Application	Typo3	Typo3	4.2.8	All	All	All
Application	Typo3	Typo3	4.2.9	All	All	All

Product	Version	Version	Version	Version	Version	Version
Application	Typo3	Typo3	4.3.0	All	All	All
Application	Typo3	Typo3	4.3.1	All	All	All
Application	Typo3	Typo3	4.3.2	All	All	All
Application	Typo3	Typo3	4.3.3	All	All	All
Application	Typo3	Typo3	4.3.4	All	All	All
Application	Typo3	Typo3	4.3.5	All	All	All
Application	Typo3	Typo3	4.3.6	All	All	All
Application	Typo3	Typo3	4.3.7	All	All	All
Application	Typo3	Typo3	4.3.8	All	All	All
Application	Typo3	Typo3	4.4.0	All	All	All
Application	Typo3	Typo3	4.4.1	All	All	All
Application	Typo3	Typo3	4.4.2	All	All	All
Application	Typo3	Typo3	4.4.3	All	All	All
Application	Typo3	Typo3	4.4.4	All	All	All
Application	Typo3	Typo3	4.2.0	All	All	All
Application	Typo3	Typo3	4.2.1	All	All	All
Application	Typo3	Typo3	4.2.10	All	All	All
Application	Typo3	Typo3	4.2.11	All	All	All
Application	Typo3	Typo3	4.2.12	All	All	All
Application	Typo3	Typo3	4.2.13	All	All	All
Application	Typo3	Typo3	4.2.14	All	All	All
Application	Typo3	Typo3	4.2.15	All	All	All
Application	Typo3	Typo3	4.2.2	All	All	All
Application	Typo3	Typo3	4.2.3	All	All	All
Application	Typo3	Typo3	4.2.4	All	All	All
Application	Typo3	Typo3	4.2.5	All	All	All
Application	Typo3	Typo3	4.2.6	All	All	All
Application	Typo3	Typo3	4.2.7	All	All	All
Application	Typo3	Typo3	4.2.8	All	All	All
Application	Typo3	Typo3	4.2.9	All	All	All
Application	Typo3	Typo3	4.3.0	All	All	All
Application	Typo3	Typo3	4.3.1	All	All	All
Application	Typo3	Typo3	4.3.2	All	All	All
Application	Typo3	Typo3	4.3.3	All	All	All
Application	Typo3	Typo3	4.3.4	All	All	All

Application	Typo3	Typo3	4.3.5	All	All	All
Application	Typo3	Typo3	4.3.6	All	All	All
Application	Typo3	Typo3	4.3.7	All	All	All
Application	Typo3	Typo3	4.3.8	All	All	All
Application	Typo3	Typo3	4.4.0	All	All	All
Application	Typo3	Typo3	4.4.1	All	All	All
Application	Typo3	Typo3	4.4.2	All	All	All
Application	Typo3	Typo3	4.4.3	All	All	All
Application	Typo3	Typo3	4.4.4	All	All	All
cpe:2.3:a:typo3:typo3:4.2.0:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.10:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.11:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.12:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.13:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.14:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.15:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.3:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.4:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.5:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.6:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.7:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.8:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.2.9:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.3.0:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.3.1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.3.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.3.3:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.3.4:*:*:*:*:*:						

cpe:2.3:a:typo3:typo3:4.3.5:*****:
cpe:2.3:a:typo3:typo3:4.3.6:*****:
cpe:2.3:a:typo3:typo3:4.3.7:*****:
cpe:2.3:a:typo3:typo3:4.3.8:*****:
cpe:2.3:a:typo3:typo3:4.4.0:*****:
cpe:2.3:a:typo3:typo3:4.4.1:*****:
cpe:2.3:a:typo3:typo3:4.4.2:*****:
cpe:2.3:a:typo3:typo3:4.4.3:*****:
cpe:2.3:a:typo3:typo3:4.4.4:*****:
cpe:2.3:a:typo3:typo3:4.2.0:*****:
cpe:2.3:a:typo3:typo3:4.2.1:*****:
cpe:2.3:a:typo3:typo3:4.2.10:*****:
cpe:2.3:a:typo3:typo3:4.2.11:*****:
cpe:2.3:a:typo3:typo3:4.2.12:*****:
cpe:2.3:a:typo3:typo3:4.2.13:*****:
cpe:2.3:a:typo3:typo3:4.2.14:*****:
cpe:2.3:a:typo3:typo3:4.2.15:*****:
cpe:2.3:a:typo3:typo3:4.2.2:*****:
cpe:2.3:a:typo3:typo3:4.2.3:*****:
cpe:2.3:a:typo3:typo3:4.2.4:*****:
cpe:2.3:a:typo3:typo3:4.2.5:*****:
cpe:2.3:a:typo3:typo3:4.2.6:*****:
cpe:2.3:a:typo3:typo3:4.2.7:*****:
cpe:2.3:a:typo3:typo3:4.2.8:*****:
cpe:2.3:a:typo3:typo3:4.2.9:*****:
cpe:2.3:a:typo3:typo3:4.3.0:*****:
cpe:2.3:a:typo3:typo3:4.3.1:*****:
cpe:2.3:a:typo3:typo3:4.3.2:*****:
cpe:2.3:a:typo3:typo3:4.3.3:*****:

cpe:2.3:a:typo3:typo3:4.3.4:*****:
cpe:2.3:a:typo3:typo3:4.3.5:*****:
cpe:2.3:a:typo3:typo3:4.3.6:*****:
cpe:2.3:a:typo3:typo3:4.3.7:*****:
cpe:2.3:a:typo3:typo3:4.3.8:*****:
cpe:2.3:a:typo3:typo3:4.4.0:*****:
cpe:2.3:a:typo3:typo3:4.4.1:*****:
cpe:2.3:a:typo3:typo3:4.4.2:*****:
cpe:2.3:a:typo3:typo3:4.4.3:*****:
cpe:2.3:a:typo3:typo3:4.4.4:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)