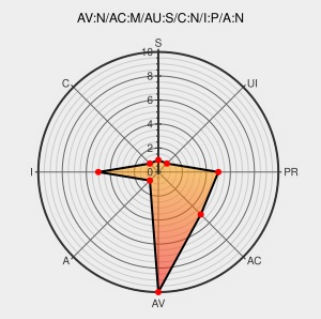
CVE-2015-5956

Published on: 09/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5956

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



Certain versions of Typo3 from Typo3 contain the following vulnerability:

The sanitizeLocalUrl function in TYPO3 6.x before 6.2.15, 7.x before 7.4.0, 4.5.40, and earlier allows remote authenticated users to bypass the XSS filter and conduct cross-site scripting (XSS) attacks via a base64 encoded data URI, as demonstrated by the (1) returnUrl parameter to show_rechis.php and the (2) redirect_url parameter to index.php.

CVE-2015-5956 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Non-Persistent Cross-Site Scripting - - TYPO3 - The Enterprise Open Source CMS	Vendor Advisory typo3.org text/html	CONFIRM typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-009/
Full Disclosure: [CVE-2015-5956] Typo3 Core sanitizeLocalUrl() Non-Persistent Cross-Site Scripting	seclists.org text/html	FULLDISC 20150915 [CVE-2015-5956] Typo3 Core sanitizeLocalUrl() Non-Persistent Cross-Site Scripting
Typo3 CMS 6.2.14 / 4.5.40 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/133551/Typo3-CMS-6.2.14-4.5.40-Cross-Site-Scripting.html
SecurityFocus	web.archive.org text/html	BUGTRAQ 20150914 [CVE-2015-5956] Typo3 Core sanitizeLocalUrl() Non-Persistent

	text/html Inactive Link Not Archived	Typo3 Core sanitizeLocalUrl() Non-Persistent Cross-Site Scripting
TYPO3 Input Validation Flaw in sanitizeLocalUrl() Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1033551

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	6.0	All	All	All
Application	Typo3	Typo3	6.0.1	All	All	All
Application	Typo3	Typo3	6.0.10	All	All	All
Application	Typo3	Typo3	6.0.11	All	All	All
Application	Typo3	Typo3	6.0.12	All	All	All
Application	Typo3	Typo3	6.0.13	All	All	All
Application	Typo3	Typo3	6.0.14	All	All	All
Application	Typo3	Typo3	6.0.2	All	All	All
Application	Typo3	Typo3	6.0.3	All	All	All
Application	Typo3	Typo3	6.0.4	All	All	All
Application	Typo3	Typo3	6.0.5	All	All	All
Application	Typo3	Typo3	6.0.6	All	All	All
Application	Typo3	Typo3	6.0.7	All	All	All
Application	Typo3	Typo3	6.0.8	All	All	All
Application	Typo3	Typo3	6.0.9	All	All	All
Application	Typo3	Typo3	6.1	All	All	All
Application	Typo3	Typo3	6.1.1	All	All	All
Application	Typo3	Typo3	6.1.2	All	All	All
Application	Typo3	Typo3	6.1.3	All	All	All
Application	Typo3	Typo3	6.1.4	All	All	All
Application	Typo3	Typo3	6.1.5	All	All	All
Application	Typo3	Typo3	6.1.6	All	All	All
Application	Typo3	Typo3	6.1.7	All	All	All
Application	Typo3	Typo3	6.1.8	All	All	All
Application	Typo3	Typo3	6.1.9	All	All	All

Application	Typo3	Typo3	6.2	All	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	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.10	All	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	6.2.2	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	7.1.0	All	All	All
Application	Typo3	Typo3	7.2.0	All	All	All
Application	Typo3	Typo3	7.3.0	All	All	All
Application	Typo3	Typo3	6.0	All	All	All
Application	Typo3	Typo3	6.0.1	All	All	All
Application	Typo3	Typo3	6.0.10	All	All	All
Application	Typo3	Typo3	6.0.11	All	All	All
Application	Typo3	Typo3	6.0.12	All	All	All
Application	Typo3	Typo3	6.0.13	All	All	All
Application	Typo3	Typo3	6.0.14	All	All	All
Application	Typo3	Typo3	6.0.2	All	All	All
Application	Typo3	Typo3	6.0.3	All	All	All
Application	Typo3	Typo3	6.0.4	All	All	All
Application	Typo3	Typo3	6.0.5	All	All	All
Application	Typo3	Typo3	6.0.6	All	All	All
Application	Typo3	Typo3	6.0.7	All	All	All

Application	Typo3	Typo3	6.0.8	All	All	All
Application	Typo3	Typo3	6.0.9	All	All	All
Application	Typo3	Typo3	6.1	All	All	All
Application	Typo3	Typo3	6.1.1	All	All	All
Application	Typo3	Typo3	6.1.2	All	All	All
Application	Typo3	Typo3	6.1.3	All	All	All
Application	Typo3	Typo3	6.1.4	All	All	All
Application	Typo3	Typo3	6.1.5	All	All	All
Application	Typo3	Typo3	6.1.6	All	All	All
Application	Typo3	Typo3	6.1.7	All	All	All
Application	Typo3	Typo3	6.1.8	All	All	All
Application	Typo3	Typo3	6.1.9	All	All	All
Application	Typo3	Typo3	6.2	All	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	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.10	All	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	6.2.2	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	7.1.0	All	All	All
Application	Typo3	Typo3	7.2.0	All	All	All
Application	Typo3	Typo3	7.3.0	All	All	All
Application	Typo3	Typo3	All	All	All	All

cpe:2.3:a:typo3:typo3:6.0:*:*:*:*:*:*:*

cpe:2.3:a:typo3:typo3:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.1.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:6.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:7.3.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→