

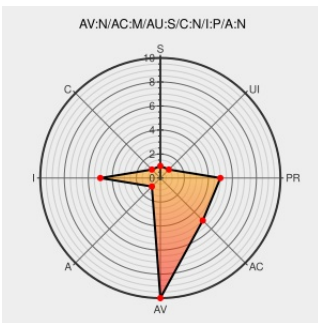


CVE-2012-6147

Published on: 07/01/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:21 PM UTC

CVE-2012-6147

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Cross-site scripting (XSS) vulnerability in the tree render API (TCA-Tree) in the Backend API in TYPO3 4.5.x before 4.5.21, 4.6.x before 4.6.14, and 4.7.x before 4.7.6 allows remote authenticated backend users to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-6147 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

oss-security - Re: Re: [Ticket#201211110000015]
TYPO3-CORE-SA-2012-005: Several Vulnerabilities in
TYPO3 Core

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

MLIST [oss-security] 20130619 Re: Re:
[Ticket#201211110000015] TYPO3-CORE-SA-
2012-005: Several Vulnerabilities in TYPO3 Core

Several Vulnerabilities in TYPO3 Core - TYPO3 - The
Enterprise Open Source CMS

[Vendor Advisory](#)
typo3.org
[text/html](#)

CONFIRM typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2012-005/

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
[text/html](#)

XF typo3-backend-treerender-xss(79967)

No Description Provided

osvdb.org

OSVDB 87113

Inactive Link **Not Archived**

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

Readers are interested to get the information shared as external source or other sites being referenced, or not, from this page. There may be other resources 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	4.5	All	All	All
Application	Typo3	Typo3	4.5.0	All	All	All
Application	Typo3	Typo3	4.5.1	All	All	All
Application	Typo3	Typo3	4.5.10	All	All	All
Application	Typo3	Typo3	4.5.11	All	All	All
Application	Typo3	Typo3	4.5.12	All	All	All
Application	Typo3	Typo3	4.5.13	All	All	All
Application	Typo3	Typo3	4.5.14	All	All	All
Application	Typo3	Typo3	4.5.15	All	All	All
Application	Typo3	Typo3	4.5.16	All	All	All
Application	Typo3	Typo3	4.5.17	All	All	All
Application	Typo3	Typo3	4.5.18	All	All	All
Application	Typo3	Typo3	4.5.19	All	All	All
Application	Typo3	Typo3	4.5.2	All	All	All
Application	Typo3	Typo3	4.5.20	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	4.5.9	All	All	All
Application	Typo3	Typo3	4.6	All	All	All
Application	Typo3	Typo3	4.6.0	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All
Application	Typo3	Typo3	4.6.10	All	All	All
Application	Typo3	Typo3	4.6.11	All	All	All
Application	Typo3	Typo3	4.6.12	All	All	All
Application	Typo3	Typo3	4.6.13	All	All	All

Application	Typo3	Typo3	4.6.2	All	All	All
Application	Typo3	Typo3	4.6.3	All	All	All
Application	Typo3	Typo3	4.6.4	All	All	All
Application	Typo3	Typo3	4.6.5	All	All	All
Application	Typo3	Typo3	4.6.6	All	All	All
Application	Typo3	Typo3	4.6.7	All	All	All
Application	Typo3	Typo3	4.6.8	All	All	All
Application	Typo3	Typo3	4.6.9	All	All	All
Application	Typo3	Typo3	4.7	All	All	All
Application	Typo3	Typo3	4.7.0	All	All	All
Application	Typo3	Typo3	4.7.1	All	All	All
Application	Typo3	Typo3	4.7.2	All	All	All
Application	Typo3	Typo3	4.7.3	All	All	All
Application	Typo3	Typo3	4.7.4	All	All	All
Application	Typo3	Typo3	4.7.5	All	All	All
Application	Typo3	Typo3	4.5	All	All	All
Application	Typo3	Typo3	4.5.0	All	All	All
Application	Typo3	Typo3	4.5.1	All	All	All
Application	Typo3	Typo3	4.5.10	All	All	All
Application	Typo3	Typo3	4.5.11	All	All	All
Application	Typo3	Typo3	4.5.12	All	All	All
Application	Typo3	Typo3	4.5.13	All	All	All
Application	Typo3	Typo3	4.5.14	All	All	All
Application	Typo3	Typo3	4.5.15	All	All	All
Application	Typo3	Typo3	4.5.16	All	All	All
Application	Typo3	Typo3	4.5.17	All	All	All
Application	Typo3	Typo3	4.5.18	All	All	All
Application	Typo3	Typo3	4.5.19	All	All	All
Application	Typo3	Typo3	4.5.2	All	All	All
Application	Typo3	Typo3	4.5.20	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	4.5.9	All	All	All
Application	Typo3	Typo3	4.6	All	All	All
Application	Typo3	Typo3	4.6.0	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All
Application	Typo3	Typo3	4.6.10	All	All	All
Application	Typo3	Typo3	4.6.11	All	All	All
Application	Typo3	Typo3	4.6.12	All	All	All
Application	Typo3	Typo3	4.6.13	All	All	All
Application	Typo3	Typo3	4.6.2	All	All	All
Application	Typo3	Typo3	4.6.3	All	All	All
Application	Typo3	Typo3	4.6.4	All	All	All
Application	Typo3	Typo3	4.6.5	All	All	All
Application	Typo3	Typo3	4.6.6	All	All	All
Application	Typo3	Typo3	4.6.7	All	All	All
Application	Typo3	Typo3	4.6.8	All	All	All
Application	Typo3	Typo3	4.6.9	All	All	All
Application	Typo3	Typo3	4.7	All	All	All
Application	Typo3	Typo3	4.7.0	All	All	All
Application	Typo3	Typo3	4.7.1	All	All	All
Application	Typo3	Typo3	4.7.2	All	All	All
Application	Typo3	Typo3	4.7.3	All	All	All
Application	Typo3	Typo3	4.7.4	All	All	All
Application	Typo3	Typo3	4.7.5	All	All	All
cpe:2.3:a:typo3:typo3:4.5:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.0:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.10:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.11:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.12:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.13:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.14:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:4.5.15:*:*:*:*:*:						

```
cpe:2.3:a:typo3:typo3:4.5.16:*:*:*:*:*:*:*:
```

cpe:2.3:a:typo3:typo3:4.5.17:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.18:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.5.19:*:*:*:*:*:*:

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

```
cpe:2.3:a:typo3:typo3:4.5.20:::*:*:*:*:*:
```

```
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:typo3:4.5.9:*:*:*:*:*:*:

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

```
cpe:2.3:a:typo3:typo3:4.6.0:*:*:*:*:*:*:*:
```

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

```
cpe:2.3:a:typo3:typo3:4.6.10:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.11:*:*:*:*:*:*:
```

cpe:2.3:a:typo3:typo3:4.6.12:*:*:*:*:*:*:

```
cpe:2.3:a:typo3:typo3:4.6.13:*:*:*:*:*:*:
```

cpe:2.3:a:typo3:typo3:4.6.2:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:4.6.3:*:*:*:*:*:*:

```
cpe:2.3:a:typo3:typo3:4.6.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:typo3:typo3:4.6.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:tvno3:tvno3:4.7:*:*:*:*:*:*:
```

cpe:2.3:a:typo3:typo3:4.7.0:*****:
cpe:2.3:a:typo3:typo3:4.7.1:*****:
cpe:2.3:a:typo3:typo3:4.7.2:*****:
cpe:2.3:a:typo3:typo3:4.7.3:*****:
cpe:2.3:a:typo3:typo3:4.7.4:*****:
cpe:2.3:a:typo3:typo3:4.7.5:*****:
cpe:2.3:a:typo3:typo3:4.5:*****:
cpe:2.3:a:typo3:typo3:4.5.0:*****:
cpe:2.3:a:typo3:typo3:4.5.1:*****:
cpe:2.3:a:typo3:typo3:4.5.10:*****:
cpe:2.3:a:typo3:typo3:4.5.11:*****:
cpe:2.3:a:typo3:typo3:4.5.12:*****:
cpe:2.3:a:typo3:typo3:4.5.13:*****:
cpe:2.3:a:typo3:typo3:4.5.14:*****:
cpe:2.3:a:typo3:typo3:4.5.15:*****:
cpe:2.3:a:typo3:typo3:4.5.16:*****:
cpe:2.3:a:typo3:typo3:4.5.17:*****:
cpe:2.3:a:typo3:typo3:4.5.18:*****:
cpe:2.3:a:typo3:typo3:4.5.19:*****:
cpe:2.3:a:typo3:typo3:4.5.2:*****:
cpe:2.3:a:typo3:typo3:4.5.20:*****:
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:typo3:4.5.9:*****:

cpe:2.3:a:typo3:typo3:4.6:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.0:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.1:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.10:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.11:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.12:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.13:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.2:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.3:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.4:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.5:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.6:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.7:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.8:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.6.9:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.0:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.1:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.2:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.3:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.4:*:*:*:*:*:
cpe:2.3:a:typo3:typo3:4.7.5:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)