



CVE-2015-8756

Published on: 01/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

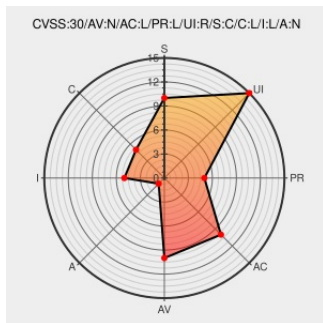
CVE-2015-8756

[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 search result view in the Indexed Search (indexed_search) component in TYPO3 6.2.x before 6.2.16 allows remote authenticated editors to inject arbitrary web script or HTML via unspecified vectors.

CVE-2015-8756 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

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
TYPO3 Input Validation Flaw in Indexed Search Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTrack 1034486
Cross-Site Scripting in TYPO3 component Indexed Search - - TYPO3 - The Enterprise Open Source CMS	Vendor Advisory typo3.org	CONFIRM typo3.org/teams/security/security-

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	6.2	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	6.2	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
cpe:2.3:a:typo3:typo3:6.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:alpha1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:alpha2:*:*:*:*:*:						

cpe:2.3:a:typo3:typo3:6.2.0:alpha3:*****:
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:typo3:6.2.0:beta4:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta5:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta6:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta7:*****:
cpe:2.3:a:typo3:typo3:6.2.0:rc1:*****:
cpe:2.3:a:typo3:typo3:6.2.0:rc2:*****:
cpe:2.3:a:typo3:typo3:6.2.1:*****:
cpe:2.3:a:typo3:typo3:6.2.10:*****:
cpe:2.3:a:typo3:typo3:6.2.10:rc1:*****:
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:typo3:6.2.15:*****:
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:typo3:6.2:*****:
cpe:2.3:a:typo3:typo3:6.2.0:alpha1:*****:

cpe:2.3:a:typo3:typo3:6.2.0:alpha2:*****:
cpe:2.3:a:typo3:typo3:6.2.0:alpha3:*****:
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:typo3:6.2.0:beta4:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta5:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta6:*****:
cpe:2.3:a:typo3:typo3:6.2.0:beta7:*****:
cpe:2.3:a:typo3:typo3:6.2.0:rc1:*****:
cpe:2.3:a:typo3:typo3:6.2.0:rc2:*****:
cpe:2.3:a:typo3:typo3:6.2.1:*****:
cpe:2.3:a:typo3:typo3:6.2.10:*****:
cpe:2.3:a:typo3:typo3:6.2.10:rc1:*****:
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:typo3:6.2.15:*****:
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:*****:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)