



CVE-2012-1608

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1608
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-04 20:55:00 UTC
Updated	2012-09-05 04:00:00 UTC
Description	The t3lib_div::RemoveXSS API method in TYPO3 4.4.0 through 4.4.13, 4.5.0 through 4.5.13, 4.6.0 through 4.6.6, 4.7, and 4.7.1-4.7.4 is vulnerable to a cross-site scripting (XSS) attack. An attacker can inject a malicious script into the page, which is then executed by the browser. This can lead to the disclosure of sensitive information, session hijacking, and other malicious actions.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	4.4.0	All	All	All
Application	Typo3	Typo3	4.4.1	All	All	All
Application	Typo3	Typo3	4.4.10	All	All	All
Application	Typo3	Typo3	4.4.11	All	All	All
Application	Typo3	Typo3	4.4.12	All	All	All
Application	Typo3	Typo3	4.4.13	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	4.4.5	All	All	All
Application	Typo3	Typo3	4.4.6	All	All	All
Application	Typo3	Typo3	4.4.7	All	All	All
Application	Typo3	Typo3	4.4.8	All	All	All
Application	Typo3	Typo3	4.4.9	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	4.5.2	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	4.5.9	All	All	All
Application	Typo3	Typo3	4.6.0	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All
Application	Typo3	Typo3	4.6.2	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	4.7	All	All	All
Application	Typo3	Typo3	6.0	All	All	All
Application	Typo3	Typo3	4.4.0	All	All	All
Application	Typo3	Typo3	4.4.1	All	All	All
Application	Typo3	Typo3	4.4.10	All	All	All
Application	Typo3	Typo3	4.4.11	All	All	All
Application	Typo3	Typo3	4.4.12	All	All	All
Application	Typo3	Typo3	4.4.13	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	4.4.5	All	All	All
Application	Typo3	Typo3	4.4.6	All	All	All
Application	Typo3	Typo3	4.4.7	All	All	All
Application	Typo3	Typo3	4.4.8	All	All	All
Application	Typo3	Typo3	4.4.9	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	4.5.2	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	4.5.9	All	All	All
Application	Typo3	Typo3	4.6.0	All	All	All
Application	Typo3	Typo3	4.6.1	All	All	All
Application	Typo3	Typo3	4.6.2	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	4.7	All	All	All
Application	Typo3	Typo3	6.0	All	All	All

References						
Reference			Source	Link	Tags	
oss-security - Re: CVE request: TYPO3-CORE-SA-2012-001			MLIST	www.openwall.com		
TYPO3 Core TYPO3-CORE-SA-2012-001 Multiple Remote Security Vulnerabilities			BID	www.securityfocus.com		
Security Advisory SA48647 - Debian update for typo3-src - Secunia			SECUNIA	secunia.com	Vendor Advisor	
Several Vulnerabilities in TYPO3 Core - TYPO3 - The Enterprise Open Source CMS			CONFIRM	typo3.org	Vendor Advisor	
80762			OSVDB	www.osvdb.org		
Debian -- Security Information -- DSA-2445-1 typo3-src			DEBIAN	www.debian.org		
CVE Program record			CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail			NVD	nvd.nist.gov	canonical, anal	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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