



CVE-2012-2112

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

Summary

CVE	CVE-2012-2112
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-27 21:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Exception Handler in TYPO3 4.4.x before 4.4.15, 4.5.x before 4.5.15, 4.6.x be

Risk And Classification

Problem Types: CWE-79

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	4.4.14	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	4.5.14	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	4.6.7	All	All	All
Application	Typo3	Typo3	4.7	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	4.4.14	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	4.5.14	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	4.6.7	All	All	All
Application	Typo3	Typo3	4.7	All	All	All

References						
Reference				Source	Link	
[TYPO3-announce] Cross-Site Scripting Vulnerability in TYPO3 Core				MLIST	lists.typo3.org	
Debian -- Security Information -- DSA-2455-1 typo3-src				DEBIAN	www.debian.org	
TYPO3 Exception Handler Cross Site Scripting Vulnerability				BID	www.securityfocus.com	
oss-security - Re: CVE-request: TYPO3-CORE-SA-2012-002 XSS in TYPO3 Core				MLIST	www.openwall.com	
oss-security - CVE-request: TYPO3-CORE-SA-2012-002 XSS in TYPO3 Core				MLIST	www.openwall.com	
Cross-Site Scripting Vulnerability in TYPO3 Core - TYPO3 - The Enterprise Open Source CMS				CONFIRM	typo3.org	
[TYPO3-announce] Announcing TYPO3 4.4.15, 4.5.15 and 4.6.8				MLIST	lists.typo3.org	

IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
Legacy QID Mappings		
996677 PHP (Composer) Security Update for typo3/cms (GHSA-qfr3-29w6-hwpg)		

© [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