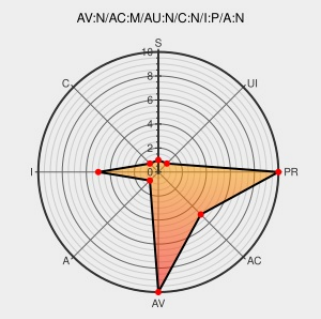
CVE-2013-7082

Published on: 12/20/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7082

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



Certain versions of Flow from Typo3 contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the errorAction method in the ActionController base class in TYPO3 Flow (formerly FLOW3) 1.1.x before 1.1.1 and 2.0.x before 2.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified input, which is returned in an error message.

CVE-2013-7082 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF typo3flow-actioncontroller-xss(89614)
Cross-Site Scripting in TYPO3 Flow - TYPO3 - The Enterprise Open Source CMS	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM typo3.org/teams/security/security-bulletins/typo3-flow/typo3-flow-sa-2013-001
Security Advisory SA55996 - TYPO3 Flow Error Messages Cross-Site Scripting Vulnerability - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 55996
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 100825

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	Flow	1.1.0	All	All	All
Application	Typo3	Flow	2.0.0	All	All	All
Application	Typo3	Flow	1.1.0	All	All	All
Application	Typo3	Flow	2.0.0	All	All	All

cpe:2.3:a:typo3:flow:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:flow:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:flow:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:flow:2.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→