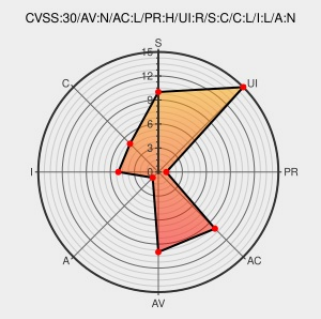
CVE-2018-6905

Published on: 04/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-6905

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



Certain versions of Typo3 from Typo3 contain the following vulnerability:

The page module in TYPO3 before 8.7.11, and 9.1.0, has XSS via $GLOBALS['TYPO3_CONF_VARS']['SYS']['sitename'], as demonstrated by an admin entering a crafted site name during the installation process.

CVE-2018-6905 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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 'sitename' Parameter Lets Remote Administrative Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1040755

GitHub - pradeepjairamani/TYPO3-XSS-POC: Typo3 -v9.1.0 Persistent Cross Site Scripting(XSS) Assigned CVE Number: CVE-2018-6905	Exploit Third Party Advisory github.com text/html	MISC github.com/pradeepjairamani/TYPO3-XSS-POC
Bug #84191: $GLOBALS['TYPO3_CONF_VARS']['SYS']['sitename'] is not properly encoded in page module - TYPO3 Core - TYPO3 Forge	Patch Vendor Advisory forge.typo3.org text/html	MISC forge.typo3.org/issues/84191

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Typo3 -v9.1.0 Persistent Cross Site Scripting(XSS) Assigned CVE Number: CVE-2018-6905

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	All	All	All	All
Application	Typo3	Typo3	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→