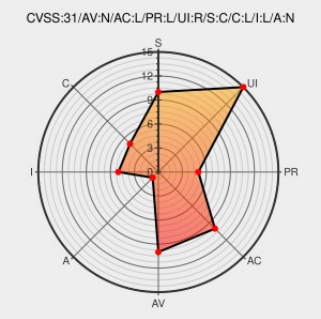
CVE-2020-11065

Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:25 PM UTC

CVE-2020-11065 - advisory for GHSA-4j77-gg36-9864

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



Certain versions of Typo3 from Typo3 contain the following vulnerability:

In TYPO3 CMS greater than or equal to 9.5.12 and less than 9.5.17, and greater than or equal to 10.2.0 and less than 10.4.2, it has been discovered that link tags generated by typolink functionality are vulnerable to cross-site scripting; properties being assigned as HTML attributes have not been parsed correctly. This has been fixed in 9.5.17 and 10.4.2.

CVE-2020-11065 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **TYPO3** - **TYPO3 CMS** version **>= 9.5.12, < 9.5.17**

Affected Vendor/Software: **TYPO3** - **TYPO3 CMS** version **>= 10.2.0, < 10.4.2**

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
Cross-Site Scripting in Link Handling · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-4j77-gg36-9864

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	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→