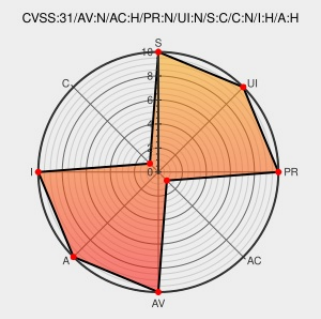
CVE-2020-11066

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

Last Modified on: 12/02/2022 07:57:00 PM UTC

CVE-2020-11066 - advisory for GHSA-2rxh-h6h9-qrqc

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 9.0.0 and less than 9.5.17 and greater than or equal to 10.0.0 and less than 10.4.2, calling unserialize() on malicious user-submitted content can lead to modification of dynamically-determined object attributes and result in triggering deletion of an arbitrary directory in the file system, if it is writable for the web server. It can also trigger message submission via email using the identity of the web site (mail relay). Another insecure deserialization vulnerability is required to actually exploit mentioned aspects. This has been fixed in 9.5.17 and 10.4.2.

CVE-2020-11066 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **TYPO3** - **TYPO3 CMS** version **>= 9.0.0, < 9.5.17**

Affected Vendor/Software: **TYPO3** - **TYPO3 CMS** version **>= 10.0.0, < 10.4.2**

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	HIGH	HIGH

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Class destructors causing side-effects when being unserialized · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-2rxh-h6h9-qrqc

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→