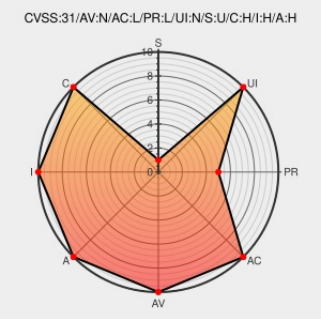
CVE-2020-11067

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

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

CVE-2020-11067 - advisory for GHSA-2wj9-434x-9hvp

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



Certain versions of Typo3 from Typo3 contain the following vulnerability:

In TYPO3 CMS 9.0.0 through 9.5.16 and 10.0.0 through 10.4.1, it has been discovered that backend user settings (in $BE_USER->uc) are vulnerable to insecure deserialization. In combination with vulnerabilities of third party components, this can lead to remote code execution. A valid backend user account is needed to exploit this vulnerability. This has been fixed in 9.5.17 and 10.4.2.

CVE-2020-11067 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH 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: 8.8 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Insecure Deserialization in Backend User Settings · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-2wj9-434x-9hvp

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→