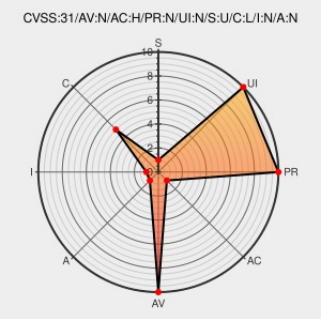
CVE-2020-11063

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

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

CVE-2020-11063 - advisory for GHSA-347x-877p-hcwx

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



Certain versions of Typo3 from Typo3 contain the following vulnerability:

In TYPO3 CMS versions 10.4.0 and 10.4.1, it has been discovered that time-based attacks can be used with the password reset functionality for backend users. This allows an attacker to mount user enumeration based on email addresses assigned to backend user accounts. This has been fixed in 10.4.2.

CVE-2020-11063 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **TYPO3** - **TYPO3 CMS** version **>= 10.4.0, <= 10.4.1**

CVSS3 Score: 3.7 - LOW

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Information Disclosure in Password Reset · Advisory ·	Third Party Advisory	CONFIRM

TYPO3/TYPO3.CMS · GitHub	github.com text/html	github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-347x-877p-hcwx

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	10.4.0	All	All	All
Application	Typo3	Typo3	10.4.1	All	All	All
Application	Typo3	Typo3	10.4.0	All	All	All
Application	Typo3	Typo3	10.4.1	All	All	All

cpe:2.3:a:typo3:typo3:10.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:10.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:10.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:10.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→