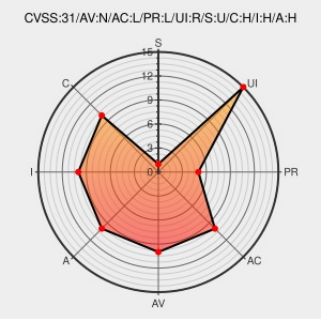
CVE-2020-11069

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

Last Modified on: 11/04/2021 05:52:00 PM UTC

CVE-2020-11069 - advisory for GHSA-pqg8-crx9-g8m4

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 the backend user interface and install tool are vulnerable to a same-site request forgery. A backend user can be tricked into interacting with a malicious resource an attacker previously managed to upload to the web server. Scripts are then executed with the privileges of the victims' user session. In a worst-case scenario, new admin users can be created which can directly be used by an attacker. The vulnerability is basically a cross-site request forgery (CSRF) triggered by a cross-site scripting vulnerability (XSS) - but happens on the same target host - thus, it's actually a same-site request forgery. Malicious payload such as HTML containing JavaScript might be provided by either an authenticated backend user or by a non-authenticated user using a third party extension, e.g. file upload in a contact form with knowing the target location. To be successful, the attacked victim requires an active and valid backend or install tool user session at the time of the attack. This has been fixed in 9.5.17 and 10.4.2. The deployment of additional mitigation techniques is suggested as described below. - Sudo Mode Extension This TYPO3 extension intercepts modifications to security relevant database tables, e.g. those storing user accounts or storages of the file abstraction layer. Modifications need to confirmed again by the acting user providing their password again. This technique is known as sudo mode. This way, unintended actions happening in the background can be mitigated. - https://github.com/FriendsOfTYPO3/sudo-mode - https://extensions.typo3.org/extension/sudo_mode - Content Security Policy Content Security Policies tell (modern) browsers how resources served a particular site are handled. It is also possible to disallow script executions for specific locations. In a TYPO3 context, it is suggested to disallow direct script execution at least for locations /fileadmin/ and /uploads/.

CVE-2020-11069 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Backend Same-Site Request Forgery · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-pqg8-crx9-g8m4

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report