



CVE-2020-26228

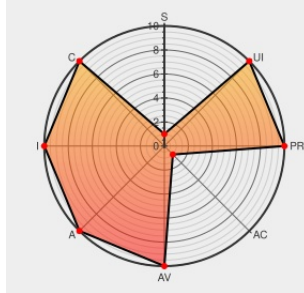
Published on: 11/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26228 - advisory for GHSA-954j-f27r-cj52

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Typo3](#) from [Typo3](#) contain the following vulnerability:

TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 9.5.23 and 10.4.10 user session identifiers were stored in cleartext - without processing with additional cryptographic hashing algorithms. This vulnerability cannot be exploited directly and occurs in combination with a chained attack - like for instance SQL injection in any other component of the system. Update to TYPO3 versions 9.5.23 or 10.4.10 that fix the problem described.

CVE-2020-26228 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **TYPO3** - **TYPO3.CMS** version $\geq 9.0.0$, $< 9.5.23$

Affected Vendor/Software: **TYPO3** - **TYPO3.CMS** version $\geq 10.0.0$, $< 10.4.10$

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description

Tags

Link

TYPO3-CORE-SA-2020-011: Cleartext storage of session identifier

Vendor Advisory

typo3.org

text/html

MISC

typo3.org/security/advisory/typo3-core-sa-2020-011

Cleartext storage of session identifier · Advisory · TYPO3/TYPO3.CMS · GitHub

Third Party Advisory

github.com

text/html

CONFIRM

github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-954j-f27r-cj52

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

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 →

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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