



CVE-2020-15098

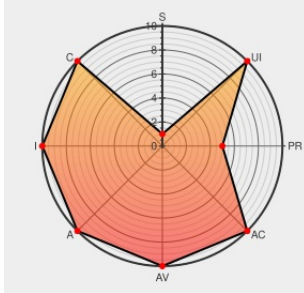
Published on: 07/29/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 06:26:00 PM UTC

CVE-2020-15098 - advisory for GHSA-m5vr-3m74-jwxxp

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

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



Certain versions of **Typo3** from **Typo3** contain the following vulnerability:

In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.20, and greater than or equal to 10.0.0 and less than 10.4.6, it has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. This allows to inject arbitrary data having a valid cryptographic message authentication code (HMAC-

SHA1) and can lead to various attack chains including potential privilege escalation, insecure deserialization & remote code execution. The overall severity of this vulnerability is high based on mentioned attack chains and the requirement of having a valid backend user session (authenticated). This has been patched in versions 9.5.20 and 10.4.6.

CVE-2020-15098 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, < 9.5.20**

Affected Vendor/Software: **TYPO3 - TYPO3 CMS** version **>= 10.0.0, 10.4.6**

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: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Avoid ambiguous HMAC results · TYPO3/TYPO3.CMS@85d3e70 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/TYPO3/TYPO3.CMS/commit/85d3e70dff35a99ef53f4b561114acfa9e5c47
TYPO3-CORE-SA-2016-013: Missing Access Check in TYPO3 CMS	Vendor Advisory typo3.org text/html	 MISC typo3.org/security/advisory/typo3-core-sa-2016-013
Sensitive Information Disclosure · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-m5vr-3m74-jwxx
TYPO3-CORE-SA-2020-008: Sensitive Information Disclosure	Vendor Advisory typo3.org text/html	 MISC typo3.org/security/advisory/typo3-core-sa-2020-008

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.

Related QID Numbers

[690526](#) Free Berkeley Software Distribution (FreeBSD) Security Update for typo3 (eab964f8-d632-11ea-9172-4c72b94353b5)

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 →](#)

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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)