



CVE-2020-26229

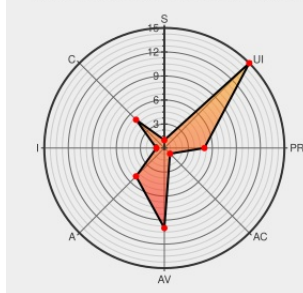
Published on: 11/23/2020 12:00:00 AM UTC

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

CVE-2020-26229 - advisory for GHSA-q9cp-mc96-m4w2

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

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



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

TYPO3 is an open source PHP based web content management system. In TYPO3 from version 10.4.0, and before version 10.4.10, RSS widgets are susceptible to XML external entity processing. This vulnerability is reasonable, but is theoretical - it was not possible to actually reproduce the vulnerability with current PHP versions of supported and maintained system distributions. At least with libxml2 version 2.9, the processing of XML external entities is disabled per default - and cannot be exploited. Besides that, a valid backend user account is needed. Update to TYPO3 version 10.4.10 to fix the problem described.

CVE-2020-26229 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **LOW** severity.

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

CVSS3 Score: **3.7 - LOW**

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

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
XML External Entity in Dashboard Widget · Advisory · TYPO3/TYPO3.CMS · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-q9cp-mc96-m4w2
TYPO3-CORE-SA-2020-012: XML External Entity in Dashboard Widget	Vendor Advisory typo3.org text/html	 MISC typo3.org/security/advisory/typo3-core-sa-2020-012

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→

© CVE.report 2023 |

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, 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