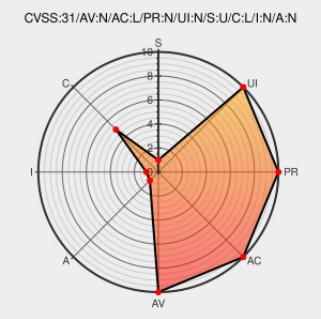
CVE-2019-10782

Published on: 01/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

CVE-2019-10782

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



Certain versions of Checkstyle from Checkstyle contain the following vulnerability:

All versions of com.puppycrawl.tools:checkstyle before 8.29 are vulnerable to XML External Entity (XXE) Injection due to an incomplete fix for CVE-2019-9658.

CVE-2019-10782 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	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
XML External Entity (XXE) Injection in com.puppycrawl.tools:checkstyle | Snyk	Exploit, Third Party Advisory, snyk.io, text/html	MISC snyk.io/vuln/SNYK-JAVA-COMPUPPYCRAWLTOOLS-543266

Pony Mail!	lists.apache.org text/html	MLIST [nifi-commits] 20200421 svn commit: r1876802 - /nifi/site/trunk/registry-security.html
[SECURITY] [DLA 2099-1] checkstyle security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200210 [SECURITY] [DLA 2099-1] checkstyle security update

Related QID Numbers

981599 Java (maven) Security Update for com.puppycrawl.tools:checkstyle (GHSA-763g-fqq7-48wg)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkstyle	Checkstyle	All	All	All	All
Application	Checkstyle	Checkstyle	All	All	All	All

cpe:2.3:a:checkstyle:checkstyle:*:*:*:*:*:*:*:*:

cpe:2.3:a:checkstyle:checkstyle:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→