



CVE-2018-18531

Published on: 10/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

CVE-2018-18531

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

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

text/impl/DefaultTextCreator.java, text/impl/ChineseTextProducer.java, and text/impl/FiveLetterFirstNameTextCreator.java in kaptcha 2.3.2 use the Random (rather than SecureRandom) function for generating CAPTCHA values, which makes it easier for remote attackers to bypass intended access restrictions via a brute-force approach.

CVE-2018-18531 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

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
Insecure Random · Issue #3 · penggle/kaptcha · GitHub	Third Party Advisory github.com text/html	MISC github.com/penggle/kaptcha/issues/3

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

981185 Java (maven) Security Update for com.github.penggle:kaptcha (GHSA-8q89-pwhh-7wfq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaptcha Project	Kaptcha	2.3.2	All	All	All
Application	Kaptcha Project	Kaptcha	2.3.2	All	All	All
cpe:2.3:a:kaptcha_project:kaptcha:2.3.2:*:*:*:*:*:						
cpe:2.3:a:kaptcha_project:kaptcha:2.3.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)