

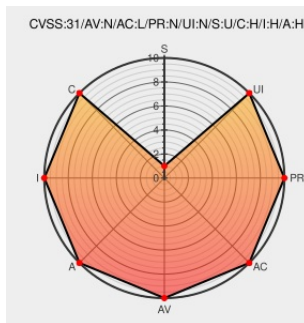


CVE-2019-16303

Published on: 09/13/2019 12:00:00 AM UTC

Last Modified on: 01/20/2023 04:31:00 PM UTC

CVE-2019-16303

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

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

A class generated by the Generator in JHipster before 6.3.0 and JHipster Kotlin through 1.1.0 produces code that uses an insecure source of randomness (apache.commons.lang3 RandomStringUtils). This allows an attacker (if able to obtain their own password reset URL) to compute the value for all other password resets for other accounts, thus allowing privilege escalation or account takeover.

CVE-2019-16303 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: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Release 6.3.0	Release Notes Vendor Advisory	MISC www.jhipster.tech/2019/09/13/jhipster-release-6.3.0.html

	www.jhipster.tech text/html	
[SECURITY] CWE-338: Vulnerability in JHipster Kotlin · Issue #183 · jhipster/jhipster-kotlin · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/jhipster/jhipster-kotlin/issues/183
Pony Mail!	lists.apache.org text/html	MLIST [commons-issues] 20200921 [jira] [Commented] (LANG-1607) To aid with CVE-2019-16303, consider upgrading RandomStringUtils default RNG
Account takeover and privilege escalation is possible in applications generated by generator-jhipster before 6.3.0. · Advisory · jhipster/generator-jhipster · GitHub	Third Party Advisory github.com text/html	MISC github.com/jhipster/generator-jhipster/security/advisories/GHSA-mwp6-j9wf-968c
Pony Mail!	lists.apache.org text/html	MLIST [commons-issues] 20200918 [jira] [Created] (LANG-1607) To aid with CVE-2019-16303, consider upgrading RandomStringUtils default RNG
Bug bounty for security advisory - thank you @JLLeitschuh · Issue #10401 · jhipster/generator-jhipster · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/jhipster/generator-jhipster/issues/10401
use new SecureRandom which uses non blocking /dev/urandom · jhipster/generator-jhipster@88448b8 · GitHub	Patch github.com text/html	MISC github.com/jhipster/generator-jhipster/commit/88448b85fd3e8e49df103f0061359037c2c68ea7
Pony Mail!	lists.apache.org text/html	MLIST [commons-issues] 20200919 [jira] [Commented] (LANG-1607) To aid with CVE-2019-16303, consider upgrading RandomStringUtils default RNG
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

[980765](#) Node.js (npm) Security Update for generator-jhipster-kotlin (GHSA-i3rh-8vwg-wh84)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhipster	Jhipster	All	All	All	All
Application	Jhipster	Jhipster	All	All	All	All
Application	Jhipster	Jhipster Kotlin	All	All	All	All
cpe:2.3:a:jhipster:jhipster:*.*.*.*.*.*.*.*.						
cpe:2.3:a:jhipster:jhipster:*.*.*.*.*.*.*.*.						
cpe:2.3:a:jhipster:jhipster_kotlin:*.*.*.*.*.*.*.*.						

No vendor comments have been submitted for this CVE

© [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](#)