

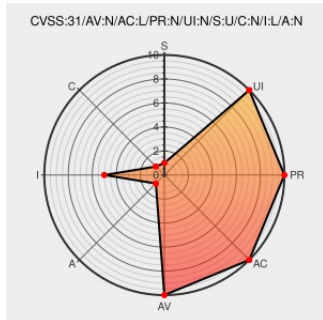


CVE-2020-4072

Published on: 06/25/2020 12:00:00 AM UTC

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

CVE-2020-4072 - advisory for GHSA-pfxf-wh96-fvjc

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

Certain versions of [Generator-jhipster-kotlin](#) from [Jhipster](#) contain the following vulnerability:

In generator-jhipster-kotlin version 1.6.0 log entries are created for invalid password reset attempts. As the email is provided by a user and the api is public this can be used by an attacker to forge log entries. This is vulnerable to <https://cwe.mitre.org/data/definitions/117.html> This problem affects only application generated with jwt or session authentication. Applications using oauth are not vulnerable. This issue has been fixed in version 1.7.0.

CVE-2020-4072 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **jhipster** - **jhipster-kotlin** version = **1.6.0**

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	NONE	LOW	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
prevent log forging when doing password reset init request · jhipster/jhipster-kotlin@426ccab · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/jhipster/jhipster-kotlin/commit/426ccab85e7e0da562643200637b99b6a2a99449
Log Injection Software Attack OWASP Foundation	Technical Description owasp.org text/html	 MISC owasp.org/www-community/attacks/Log_Injection
Log Forging Vulnerability · Advisory · jhipster/jhipster-kotlin · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/jhipster/jhipster-kotlin/security/advisories/GHSA-pxf-fvj-c
JVM Log Forging Baeldung	Technical Description www.baeldung.com text/html	 MISC www.baeldung.com/jvm-log-forging
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
983181 Nodejs (npm) Security Update for generator-jhipster-kotlin (GHSA-pxf-fvj-c)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhipster	Generator-jhipster-kotlin	All	All	All	All
Application	Jhipster	Generator-jhipster-kotlin	All	All	All	All
cpe:2.3:a:jhipster:generator-jhipster-kotlin:*:*:*:*:*:						
cpe:2.3:a:jhipster:generator-jhipster-kotlin:*:*:*:*:*:						

No vendor comments have been submitted for this CVE
← Previous ID Next ID →