



CVE-2020-25023

Published on: 09/03/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-25023

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

Certain versions of [Noise-java](#) from [Noise-java Project](#) contain the following vulnerability:

An issue was discovered in Noise-Java through 2020-08-27. AESGCMOnCtrCipherState.encryptWithAd() allows out-of-bounds access.

CVE-2020-25023 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
Full Disclosure: Noise-Java AESGCMOnCtrCipherState.encryptWithAd() insufficient boundary checks	Third Party Advisory seclists.org text/html	FULLDISC 20200904 Noise-Java AESGCMOnCtrCipherState.encryptWithAd() insufficient boundary checks
Improve array bounds checks in CipherState	Patch	MISC github.com/rweather/noise-

implementations · rweather/noise-java@18e86b6 · GitHub

Third Party Advisory

github.com

text/html

java/commit/18e86b6f8bea7326934109aa9ffa705ebf4bde90

Noise-Java
AESGCMOnCtrCipherState.encryptWithAd()
Insufficient Boundary Checks ≈ Packet Storm

Third Party Advisory

packetstormsecurity.com

text/html

MISC packetstormsecurity.com/files/159056/Noise-Java-AESGCMOnCtrCipherState.encryptWithAd-Insufficient-Boundary-Checks.html

Boundary checks improvement: detect when
plaintextOffset + length is greater than length by
polivar3 · Pull Request #12 · rweather/noise-java · GitHub

Third Party Advisory

github.com

text/html

CONFIRM github.com/rweather/noise-java/pull/12

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	Noise-java Project	Noise-java	All	All	All	All

cpe:2.3:a:noise-java_project:noise-java:*****:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →