



CVE-2020-25022

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

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

CVE-2020-25022

[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. AESGCMFallbackCipherState.encryptWithAd() allows out-of-bounds access.

CVE-2020-25022 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 AESGCMFallbackCipherState.encryptWithAd() insufficient boundary checks	Third Party Advisory seclists.org text/html	FULLDISC 20200904 Noise-Java AESGCMFallbackCipherState.encryptWithAd() insufficient boundary checks
Noise-Java	Third Party Advisory	MISC packetstormsecurity.com/files/159055/Noise-Java-

AESGCMFallbackCipherState.encryptWithAd()
Insufficient Boundary Checks ≈ Packet Storm

packetstormsecurity.com

text/html

AESGCMFallbackCipherState.encryptWithAd-Insufficient-
Boundary-Checks.html

Improve array bounds checks in CipherState
implementations · rweather/noise-java@18e86b6 ·
GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/rweather/noise-
java/commit/18e86b6f8bea7326934109aa9ffa705ebf4bde90

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 →

© 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](#)