



# CVE-2023-43642

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-43642
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-25 20:15:00 UTC
<b>Updated</b>	2023-09-26 15:46:00 UTC
<b>Description</b>	snappy-java is a Java port of the snappy, a fast C++ compressor/decompresser developed by Google. The SnappyInputStr

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xerial	Snappy-java	All	All	All	All

## References

### Reference

- Missing upper bound check on chunk length in snappy-java can lead to Denial of Service (DoS) impact · Advisory · xerial/snappy-java · GitHub
- Merge pull request from GHSA-55g7-9cww-5qfv · xerial/snappy-java@9f8c3cf · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- [20391](#) IBM DB2 Denial of Service (DoS) Vulnerability (7087234)
- [379560](#) Atlassian Bitbucket Data Center and Server org.xerial.snappy:snappy-java Dependency Denial of Service (DoS) Vulnerability (BSERV-19100)
- [731311](#) Atlassian Jira Software Data Center and Server Denial of Service (DoS) Vulnerability (JSWSERVER-25791)
- [995402](#) Java (Maven) Security Update for org.xerial.snappy:snappy-java (GHSA-55g7-9cww-5qfv)

© [CVE.report](#) 2026 |

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](#)**