



CVE-2023-28867

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

Summary

CVE	CVE-2023-28867
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-27 01:15:00 UTC
Updated	2023-04-03 14:01:00 UTC
Description	In GraphQL Java (aka graphql-java) before 20.1, an attacker can send a crafted GraphQL query that causes stack consum

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Graphql-java	Graphql-java	All	All	All	All
Application	Graphql-java	Graphql-java	20.0	All	All	All

References

Reference
Release 17.5 · graphql-java/graphql-java · GitHub
Release 18.4 · graphql-java/graphql-java · GitHub
Release 19.4 · graphql-java/graphql-java · GitHub
Preventing stack overflow exceptions via limiting the depth of the parser rules by bbakerman · Pull Request #3112 · graphql-java/graphql-java
Release 20.1 · graphql-java/graphql-java · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378729](#) IBM WebSphere Application Server Liberty Denial of Service (DoS) Vulnerability (6999681)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)