



CVE-2023-38976

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

Summary

CVE	CVE-2023-38976
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-21 17:15:00 UTC
Updated	2023-08-29 22:15:00 UTC
Description	An issue in weaviate v.1.20.0 allows a remote attacker to cause a denial of service via the handleUnbatchedGraphQLRequ

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Weaviate	Weaviate	1.20.0	All	All	All

References

Reference	Source	Link
panic when type assertions in function handleUnbatchedGraphQLRequest · Issue #3258 · weaviate/weaviate · GitHub	MISC	github.com
Notion – The all-in-one workspace for your notes, tasks, wikis, and databases.	MISC	aisec.to
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[994944](#) GO (Go) Security Update for github.com/weaviate/weaviate (GHSA-ch6w-mc6c-g65g)

[994965](#) GO (Go) Security Update for github.com/weaviate/weaviate (GHSA-8697-479h-5mfp)

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](#)