CVE-2020-8661

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8661
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-04 21:15:00 UTC
Updated	2022-05-24 18:44:00 UTC
Description	CNCF Envoy through 1.13.0 may consume excessive amounts of memory when responding internally to pipelined requests

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cncf	Envoy	All	All	All	All
Application	Redhat	Openshift Service Mesh	1.0.9	All	All	All

References

Reference	Source	Link	Tags
Response flooding for HTTP/1.1 · Advisory · envoyproxy/envoy · GitHub	MISC	github.com	Third Party Advisory
Version history — envoy tag-v1.13.1 documentation	CONFIRM	www.envoyproxy.io	Release Notes, Third Party Adv
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report