



# CVE-2022-25857

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

## Summary

<b>CVE</b>	CVE-2022-25857
<b>State</b>	PUBLIC
<b>Assigner</b>	report@snyk.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-30 05:15:00 UTC
<b>Updated</b>	2024-03-15 11:15:00 UTC
<b>Description</b>	The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial of Service (DoS) due missing to nested c

## Risk And Classification

**Problem Types:** CWE-776

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	Debian Linux	10.0	All	All	All
Application	<a href="#">Snakeyaml Project</a>	Snakeyaml	All	All	All	All

## References

Reference	Source	Link
Denial of Service (DoS) in org.yaml:snakeyaml   CVE-2022-25857   Snyk	CONFIRM	<a href="#">security.snyk.com</a>
<a href="#">security.netapp.com/advisory/ntap-20240315-0010</a>		<a href="#">security.netapp.com</a>
Restrict nested depth for collections to avoid DoS attacks · snakeyaml/snakeyaml@fc30078 · GitHub	CONFIRM	<a href="#">github.com</a>
snakeyaml / snakeyaml / issues / #525 - Got StackOverflowError for many open unmatched brackets — Bitbucket	CONFIRM	<a href="#">bitbucket.org</a>
[SECURITY] [DLA 3132-1] snakeyaml security update	MLIST	<a href="#">lists.debian.org</a>
snakeyaml / snakeyaml / commit / fc300780da21 — Bitbucket	CONFIRM	<a href="#">bitbucket.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** unknown

## Legacy QID Mappings

160132	Oracle Enterprise Linux Security Update for prometheus-jmx-exporter (ELSA-2022-6820)
181092	Debian Security Update for snakeyaml (DLA 3132-1)
182649	Debian Security Update for snakeyaml (CVE-2022-25857)
199232	Ubuntu Security Notification for SnakeYAML Vulnerabilities (USN-5944-1)
20396	IBM DB2 Multiple Vulnerabilities (7095807)
240711	Red Hat Update for JBoss Enterprise Application Platform 7.4.7 (RHSA-2022:6822)
240712	Red Hat Update for JBoss Enterprise Application Platform 7.4.7 (RHSA-2022:6823)
240713	Red Hat Update for JBoss Enterprise Application Platform 7.4.7 (RHSA-2022:6821)
240715	Red Hat Update for prometheus-jmx-exporter (RHSA-2022:6820)
241180	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:0560)
241214	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2023:0777)
241405	Red Hat Update for Satellite 6.13 (RHSA-2023:2097)
354804	Amazon Linux Security Advisory for snakeyaml : ALAS2-2023-1976
377909	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJAN2023)
378100	IBM MQ Blockchain Bridge Vulnerability (6952185)
691024	Free Berkeley Software Distribution (FreeBSD) Security Update for cassandra3 (53caf29b-9180-11ed-acbe-b42e991fc52e)
753357	SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2022:3397-1)
770173	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:0560)
770178	Red Hat OpenShift Container Platform 4.9. Security Update (RHSA-2023:0777)
903847	Common Base Linux Mariner (CBL-Mariner) Security Update for snakeyaml (10742)
940655	AlmaLinux Security Update for prometheus-jmx-exporter (ALSA-2022:6820)
960203	Rocky Linux Security Update for prometheus-jmx-exporter (RLSA-2022:6820)
960924	Rocky Linux Security Update for Satellite (RLSA-2023:2097)

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](#)