



# CVE-2022-38750

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

## Summary

<b>CVE</b>	CVE-2022-38750
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-05 10:15:00 UTC
<b>Updated</b>	2024-03-15 11:15:00 UTC
<b>Description</b>	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is run

## Risk And Classification

**Problem Types:** CWE-787

## 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	Tags
snakeyaml: Multiple Vulnerabilities (GLSA 202305-28) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
<a href="https://security.netapp.com/advisory/ntap-20240315-0010">security.netapp.com/advisory/ntap-20240315-0010</a>		<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] [DLA 3132-1] snakeyaml security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
47027 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	<a href="https://bugs.chromium.org">bugs.chromium.org</a>	
snakeyaml / snakeyaml / issues / #526 - Stackoverflow [OSS-Fuzz - 47027] — Bitbucket	MISC	<a href="https://bitbucket.org">bitbucket.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181092](#) Debian Security Update for snakeyaml (DLA 3132-1)

<a href="#">182029</a> Debian Security Update for snakeyaml (CVE-2022-38750)
<a href="#">199232</a> Ubuntu Security Notification for SnakeYAML Vulnerabilities (USN-5944-1)
<a href="#">20396</a> IBM DB2 Multiple Vulnerabilities (7095807)
<a href="#">241405</a> Red Hat Update for Satellite 6.13 (RHSA-2023:2097)
<a href="#">355419</a> Amazon Linux Security Advisory for snakeyaml : ALAS2023-2023-200
<a href="#">710729</a> Gentoo Linux snakeyaml Multiple Vulnerabilities (GLSA 202305-28)
<a href="#">753357</a> SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2022:3397-1)
<a href="#">903844</a> Common Base Linux Mariner (CBL-Mariner) Security Update for snakeyaml (10894)
<a href="#">960924</a> Rocky Linux Security Update for Satellite (RLSA-2023:2097)

© [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](#)**