



# CVE-2022-41854

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

## Summary

<b>CVE</b>	CVE-2022-41854
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-11 13:15:00 UTC
<b>Updated</b>	2024-03-15 11:15:00 UTC
<b>Description</b>	Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser i

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Snakeyaml Project</a>	<a href="#">Snakeyaml</a>	All	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] Fedora 36 Update: snakeyaml-1.32-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: snakeyaml-1.32-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 38 Update: picocli-4.7.4-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: snakeyaml-1.32-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
50355 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	CONFIRM	<a href="https://bugs.chromium.org">bugs.chromium.org</a>	
security.netapp.com/advisory/ntap-20240315-0009		<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 38 Update: picocli-4.7.4-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: snakeyaml-1.32-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

181586	Debian Security Update for snakeyaml (CVE-2022-41854)
20396	IBM DB2 Multiple Vulnerabilities (7095807)
241301	Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:1512)
241302	Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 8 (RHSA-2023:1513)
241303	Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:1514)
283543	Fedora Security Update for snakeyaml (FEDORA-2022-c01dd659fa)
283544	Fedora Security Update for snakeyaml (FEDORA-2022-8a4e8aa190)
284302	Fedora Security Update for picocli (FEDORA-2023-27ec59a486)
356386	Amazon Linux Security Advisory for snakeyaml : ALAS2023-2023-375
379452	IBM Cognos Analytics Multiple Vulnerabilities (7123154)
904485	Common Base Linux Mariner (CBL-Mariner) Security Update for snakeyaml (11427)

© [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](#)