



CVE-2017-18640

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

Summary

CVE	CVE-2017-18640
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-12 03:15:00 UTC
Updated	2023-11-07 02:41:00 UTC
Description	The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-

Risk And Classification

Problem Types: CWE-776

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Oracle	Peoplesoft Enterprise Pt Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Pt Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Pt Peopletools	8.58	All	All	All
Application	Quarkus	Quarkus	All	All	All	All
Application	Snakeyaml Project	Snakeyaml	All	All	All	All
Application	Snakeyaml Project	Snakeyaml	All	All	All	All

References

Reference

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

snakeyaml: Multiple Vulnerabilities (GLSA 202305-28) — Gentoo security

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] Fedora 32 Update: snakeyaml-1.26-1.fc32 - package-announce - Fedora Mailing-Lists

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Maven Repository: org.yaml » snakeyaml » 1.25 (Usages)

[SECURITY] Fedora 31 Update: snakeyaml-1.26-1.fc31 - package-announce - Fedora Mailing-Lists

Pony Mail!

asomov / snakeyaml / wiki / Billion laughs attack — Bitbucket

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

snakeyaml / snakeyaml / issues / #377 - Allow configuration for preventing billion laughs attack — Bitbucket

asomov / snakeyaml / issues / #377 - Allow configuration for preventing billion laughs attack — Bitbucket

Pony Mail!

[kafka-users] 20210617 vulnerabilities

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

snakeyaml / snakeyaml / wiki / Changes — Bitbucket

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

20269 IBM DB2 Multiple Vulnerabilities (6466365)
375482 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2021)
710729 Gentoo Linux snakeyaml Multiple Vulnerabilities (GLSA 202305-28)
750114 SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2021:1876-1)
750651 SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2021:1979-1)
750653 SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2021:1978-1)
750775 OpenSUSE Security Update for snakeyaml (openSUSE-SU-2021:1876-1)
900938 Common Base Linux Mariner (CBL-Mariner) Security Update for snakeyaml (7359)
940262 AlmaLinux Security Update for prometheus-jmx-exporter (ALSA-2020:4807)
960673 Rocky Linux Security Update for prometheus-jmx-exporter (RLSA-2020:4807)
980460 Java (maven) Security Update for org.yaml:snakeyaml (GHSA-rvwf-54qp-4r6v)

© [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](#)