CVE-2022-1471

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1471
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-01 11:15:00 UTC
Updated	2023-11-19 15:15:00 UTC
Description	SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snakeyaml Project	Snakeyaml	All	All	All	All
Application	Snakeyaml Project	Snakeyaml	1.30	All	All	All

References

Reference	Source	Link
[Kubernetes Java Client] Kubernetes Java client impacted by CVE-2022-1471	MISC	groups.google.
CVE-2022-1471 SnakeYAML Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp
snakeyaml / snakeyaml / issues / #561 - CVE-2022-1471 (vulnerability in deserialization) — Bitbucket	MISC	bitbucket.org
www.openwall.com/lists/oss-security/2023/11/19/1		www.openwall
PyTorch Model Server Registration / Deserialization Remote Code Execution ≈ Packet Storm	MISC	packetstormse
www.github.com/mbechler/marshalsec/blob/master/marshalsec.pdf	MISC	www.github.co
SnakeYaml: Constructor Deserialization Remote Code Execution · Advisory · google/security-research · GitHub	MISC	github.com
GitHub - mbechler/marshalsec	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160363 Oracle Enterprise Linux Security Update for prometheus-jmx-exporter (ELSA-2022-9058-1)

20342 Oracle Database 21c Critical Patch Update - April 2023

20396 IBM DB2 Multiple Vulnerabilities (7095807)

241019 Red Hat Update for prometheus-jmx-exporter (RHSA-2022:9058)

241186 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:0697)

241214 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2023:0777)

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)

241405 Red Hat Update for Satellite 6.13 (RHSA-2023:2097)

379104 Atlassian Data Center and Server Remote Code Execution (RCE) Vulnerabilities (JSWSERVER-24756)

379105 Atlassian Bitbucket Data Center Remote Code Execution (RCE) Vulnerability (BSERV-14528)

379149 Atlassian Jira Service Management Server and Data Center Remote Code Execution (RCE) Vulnerability (JSDSERVER-14906)

379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)

520012 Atlassian Bitbucket Data Center and Server Remote Code Execution (CVE-2022-1471)

731000 Atlassian Confluence Data Center and Server Remote Code Execution (RCE) Vulnerability (CONFSERVER-91463)

731002 Atlassian Bitbucket Server Remote Code Execution (RCE) Vulnerability (BSERV-14528)

731035 Atlassian Data Center and Server Remote Code Execution (RCE) Vulnerabilities (JSWSERVER-24756)

770175 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:0697)

770178 Red Hat OpenShift Container Platform 4.9. Security Update (RHSA-2023:0777)

940858 AlmaLinux Security Update for prometheus-jmx-exporter (ALSA-2022:9058)

960565 Rocky Linux Security Update for prometheus-jmx-exporter (RLSA-2022:9058)

960924 Rocky Linux Security Update for Satellite (RLSA-2023:2097)

996013 Python (Pip) Security Update for apache-submarine (GHSA-8hcr-5x2g-9f7j)

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