



CVE-2022-31115

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

Summary

CVE	CVE-2022-31115
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-30 22:15:00 UTC
Updated	2022-07-25 09:34:00 UTC
Description	opensearch-ruby is a community-driven, open source fork of elasticsearch-ruby. In versions prior to 2.0.1 the ruby `YAML.load` method is used to parse YAML documents. This method is known to be vulnerable to remote code execution (RCE) via a specially crafted YAML document. The vulnerability is caused by the use of the `YAML.load` method, which is known to be vulnerable to RCE via a specially crafted YAML document. The vulnerability is caused by the use of the `YAML.load` method, which is known to be vulnerable to RCE via a specially crafted YAML document.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Opensearch	All	All	All	All
Application	Opensearch	Opensearch	All	All	All	All

References

Reference	Source	Link
Universal RCE with Ruby YAML.load (versions > 2.7) - Staalraad	MISC	staal
Use safe_load instead of load for yaml by VachaShah · Pull Request #77 · opensearch-project/opensearch-ruby · GitHub	MISC	github
Unsafe YAML deserialization in Ruby Client · Advisory · opensearch-project/opensearch-ruby · GitHub	CONFIRM	github
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)