



CVE-2022-3064

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-3064 |
| State | PUBLIC |
| Assigner | security@golang.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-12-27 22:15:00 UTC |
| Updated | 2023-09-15 21:15:00 UTC |
| Description | Parsing malicious or large YAML documents can consume excessive amounts of CPU or memory. |

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------------|----------------------|---------|--------|---------|----------|
| Application | Yaml Project | Yaml | All | All | All | All |

References

| Reference | Source | Link |
|--|---------|---|
| [SECURITY] Fedora 39 Update: moby-engine-24.0.5-1.fc39 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| [SECURITY] Fedora 38 Update: moby-engine-24.0.5-1.fc38 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| [SECURITY] Fedora 37 Update: exercism-3.2.0-1.fc37 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| [SECURITY] Fedora 37 Update: moby-engine-24.0.5-1.fc37 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| [SECURITY] [DLA 3479-1] golang-yaml.v2 security update | MISC | lists.debian.org |
| [SECURITY] Fedora 38 Update: exercism-3.2.0-1.fc38 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| Release v2.2.4: Improve heuristics preventing CPU/memory abuse (#515) · go-yaml/yaml · GitHub | MISC | github.com |
| GO-2022-0956 - Go Packages | MISC | pkg.go.dev |
| [SECURITY] Fedora 39 Update: exercism-3.2.0-1.fc39 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org |
| Improve heuristics preventing CPU/memory abuse (#515) · go-yaml/yaml@f221b84 · GitHub | 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

| | |
|---------|--|
| 161175 | Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2023-6939) |
| 161187 | Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2023-6938) |
| 181573 | Debian Security Update for golang-yaml.v2 (CVE-2022-3064) |
| 199656 | Ubuntu Security Notification for Go yaml Vulnerabilities (USN-6287-1) |
| 241230 | Red Hat Update for OpenStack Platform 17.0 (RHSA-2023:1014) |
| 241268 | Red Hat Update for multiple OpenStack Platforms (RHSA-2023:1275) |
| 242288 | Red Hat Update for toolbox (RHSA-2023:6346) |
| 242415 | Red Hat Update for container-tools:rhel8 (RHSA-2023:6939) |
| 242458 | Red Hat Update for container-tools:4.0 (RHSA-2023:6938) |
| 283781 | Fedora Security Update for manifest (FEDORA-2023-11dafed208) |
| 283782 | Fedora Security Update for manifest (FEDORA-2023-a4baceec07) |
| 283815 | Fedora Security Update for gmailctl (FEDORA-2023-ca444fdecf) |
| 283816 | Fedora Security Update for gmailctl (FEDORA-2023-abb47e24d8) |
| 284244 | Fedora Security Update for gmailctl (FEDORA-2023-8c02aee138) |
| 284258 | Fedora Security Update for manifest (FEDORA-2023-5312f6200c) |
| 285289 | Fedora Security Update for moby (FEDORA-2023-b9c1d0e4c5) |
| 285292 | Fedora Security Update for exercism (FEDORA-2023-e16469fdec) |
| 379641 | Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050) |
| 6000135 | Debian Security Update for golang-yaml.v2 (DLA 3479-1) |
| 904825 | Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (12324) |
| 905156 | Common Base Linux Mariner (CBL-Mariner) Security Update for application-gateway-kubernetes-ingress (12460) |
| 905210 | Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (12906) |
| 905223 | Common Base Linux Mariner (CBL-Mariner) Security Update for application-gateway-kubernetes-ingress (12928) |
| 905268 | Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (12906) |
| 905404 | Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (12906-1) |
| 906791 | Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (12906-3) |

[941391](#) AlmaLinux Security Update for toolbox (ALSA-2023:6346)

[941444](#) AlmaLinux Security Update for container-tools:4.0 (ALSA-2023:6938)

[941481](#) AlmaLinux Security Update for container-tools:rhel8 (ALSA-2023:6939)

© [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](#)