



CVE-2020-28362

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-28362 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-11-18 17:15:00 UTC |
| Updated | 2023-11-07 03:21:00 UTC |
| Description | Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service. |

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|---|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Golang | Go | All | All | All | All |
| Application | Golang | Go | All | All | All | All |
| Application | Netapp | Cloud Insights Telegraf Agent | - | All | All | All |
| Application | Netapp | Cloud Insights Telegraf Agent | - | All | All | All |
| Application | Netapp | Trident | - | All | All | All |
| Application | Netapp | Trident | - | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|--------|
| Security Advisory 0062 - Arista | MISC | www.arista.com | |
| Pony Mail! | | lists.apache.org | |
| November 2020 Golang Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | Threat |
| [SECURITY] Fedora 32 Update: golang-1.14.13-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |
| [SECURITY] Fedora 33 Update: golang-1.15.5-1.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org | |

| | | | | |
|--|---------|--|---|-----|
| [SECURITY] Fedora 33 Update: golang-1.15.5-1.fc33 - package-announce - Fedora Mailing-Lists | | | lists.fedoraproject.org | |
| Pony Mail! | MLIST | | lists.apache.org | Ma |
| [SECURITY] Fedora 32 Update: golang-1.14.13-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | | lists.fedoraproject.org | Thi |
| [SECURITY] Fedora 33 Update: golang-1.15.5-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | | lists.fedoraproject.org | Thi |
| [security] Go 1.15.5 and Go 1.14.12 are released | CONFIRM | | groups.google.com | Rel |
| CVE Program record | CVE.ORG | | www.cve.org | car |
| NVD vulnerability detail | NVD | | nvd.nist.gov | car |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [239272](#) Red Hat Update for OpenShift Container Platform 4.7.9 packages and (RHSA-2021:1366)
- [239359](#) Red Hat Update for OpenShift Container Platform 4.7.11 (RHSA-2021:1551)
- [352291](#) Amazon Linux Security Update for golang: AL2012-2021-332
- [501574](#) Alpine Linux Security Update for go
- [690435](#) Free Berkeley Software Distribution (FreeBSD) Security Update for go (db4b2f27-252a-11eb-865c-00155d646400)
- [750526](#) OpenSUSE Security Update for go1.15 (openSUSE-SU-2020:2139-1)
- [750544](#) OpenSUSE Security Update for go1.14 (openSUSE-SU-2020:2067-1)
- [750559](#) OpenSUSE Security Update for go1.14 (openSUSE-SU-2020:2047-1)
- [770048](#) Red Hat OpenShift Container Platform 4.6.12 Packages and Security Update (RHSA-2021:0038)
- [770053](#) Red Hat OpenShift Container Platform 4.6.23 Security Update (RHSA-2021:0956)
- [770058](#) Red Hat OpenShift Container Platform 4.7.9 Packages and Security Update (RHSA-2021:1366)
- [770059](#) Red Hat OpenShift Container Platform 4.7.11 Security and Bug Fix Update (RHSA-2021:1551)
- [770064](#) Red Hat OpenShift Container Platform 4.7.0 Packages and Security Update (RHSA-2020:5634)
- [770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)
- [770076](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0172)
- [770091](#) Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1366)
- [770105](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-0038)
- [770112](#) Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1551)
- [770116](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-0172)
- [770118](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-0956)

900148 CBL-Mariner Linux Security Update for golang 1.13.15

902816 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3604)

907752 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3604-1)

940378 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2020:5493)

© [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](#)