



CVE-2021-31525

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-31525 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-05-27 13:15:00 UTC |
| Updated | 2023-11-07 03:34:00 UTC |
| Description | net/http in Go before 1.15.12 and 1.16.x before 1.16.4 allows remote attackers to cause a denial of service (panic) via a large request. |

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Application | Golang | Go | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|---|
| Go 1.16.4 and Go 1.15.12 are released | MISC | groups.io |
| net/http: ReadRequest can stack overflow due to recursion with very large headers · Issue #45710 · golang/go · GitHub | MISC | github.com |
| Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security | GENTOO | security.gentoo.org |
| [SECURITY] Fedora 34 Update: golang-1.16.4-1.fc34 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 34 Update: golang-1.16.4-1.fc34 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| 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

159347 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-3076)

| | |
|--------|---|
| 179725 | Debian Security Update for golang-1.15golang-golang-x-net (CVE-2021-31525) |
| 239537 | Red Hat Update for OpenShift Container Platform 4.8.4 (RHSA-2021:2984) |
| 239549 | Red Hat Update for go-toolset:rhel8 (RHSA-2021:3076) |
| 239606 | Red Hat Update for OpenShift Container Platform 4.8.9 packages (RHSA-2021:3248) |
| 239641 | Red Hat Update for Red Hat OpenStack Platform 16.2 (etcd) (RHSA-2021:3487) |
| 239942 | Red Hat Update for OpenStack Platform 16.1 (RHSA-2021:5072) |
| 239945 | Red Hat Update for OpenStack Platform 16.1 |
| 239948 | Red Hat Update for OpenStack Platform 16.1 |
| 239951 | Red Hat Update for OpenStack Platform 16.1 |
| 239956 | Red Hat Update for OpenStack Platform 16.1 |
| 239957 | Red Hat Update for OpenStack Platform 16.1 |
| 240042 | Red Hat Update for openshift container storage 3.11.z (RHSA-2022:0308) |
| 281175 | Fedora Security Update for golang (FEDORA-2021-a50122f73b) |
| 352397 | Amazon Linux Security Advisory for golang: ALAS2-2021-1657 |
| 352479 | Amazon Linux Security Advisory for golang: ALAS-2021-1512 |
| 352538 | Amazon Linux Security Advisory for golang: AL2012-2021-342 |
| 375598 | Go Denial Of Service Vulnerability |
| 377560 | Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0060) |
| 378883 | Splunk Enterprise August Third Party Package Updates (SVD-2023-0808) |
| 501569 | Alpine Linux Security Update for go |
| 501858 | Alpine Linux Security Update for go |
| 670704 | EulerOS Security Update for golang (EulerOS-SA-2021-2462) |
| 670739 | EulerOS Security Update for golang (EulerOS-SA-2021-2497) |
| 670769 | EulerOS Security Update for golang (EulerOS-SA-2021-2527) |
| 670793 | EulerOS Security Update for golang (EulerOS-SA-2021-2551) |
| 670874 | EulerOS Security Update for golang (EulerOS-SA-2021-2551) |
| 690147 | Free Berkeley Software Distribution (FreeBSD) Security Update for go (7f242313-aea5-11eb-8151-67f74cf7c704) |
| 710584 | Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02) |

| |
|--|
| 750681 SUSE Enterprise Linux Security Update for go1.15 (SUSE-SU-2021:2082-1) |
| 750682 SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2021:2085-1) |
| 750703 OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:0904-1) |
| 770070 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2984) |
| 770078 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3248) |
| 770102 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-3248) |
| 770106 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2984) |
| 900141 CBL-Mariner Linux Security Update for golang 1.15.11 |
| 903273 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (4319) |
| 907762 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (4319-1) |
| 940126 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:3076) |
| 960708 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:3076) |

© [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](#)