



CVE-2020-16845

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

Summary

CVE	CVE-2020-16845
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-06 18:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Golang	Go	All	All	All	All
Application	Golang	Go	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link
-----------	--------	------

Debian -- Security Information -- DSA-4848-1 golang-1.11	DEBIAN	www.debian.org
Google Groups		groups.google.com
Google Groups		groups.google.com
[SECURITY] Fedora 32 Update: golang-1.14.7-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: golang-github-ulikunitz-xz-0.5.8-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: golang-1.14.7-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:1405-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 31 Update: golang-github-ulikunitz-xz-0.5.8-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2460-1] golang-1.8 security update	MLIST	lists.debian.org
[security-announce] openSUSE-SU-2020:1178-1: moderate: Security update f	SUSE	lists.opensuse.org
CVE-2020-16845 Golang Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Google Groups	CONFIRM	groups.google.com
[SECURITY] Fedora 31 Update: golang-github-ulikunitz-xz-0.5.8-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 2459-1] golang-1.7 security update	MLIST	lists.debian.org
[SECURITY] Fedora 31 Update: golang-1.13.15-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: golang-1.13.15-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:1407-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 32 Update: golang-github-ulikunitz-xz-0.5.8-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com
Google Groups	MISC	groups.google.com
[security-announce] openSUSE-SU-2020:1194-1: moderate: Security update f	SUSE	lists.opensuse.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

[199026](#) Ubuntu Security Notification for Go Vulnerability (USN-5725-1)

[199493](#) Ubuntu Security Notification for Go Vulnerability (USN-5725-2)

[239198](#) Red Hat Update for OpenShift Container Platform 4.6.23 (RHSA-2021:0956)

[239200](#) Red Hat Update for OpenShift Container Platform 4.5.34 packages and (RHSA-2021:0713)

[239226](#) Red Hat Update for OpenShift Container Platform 4.5.37 (RHSA-2021:1016)

[239272](#) Red Hat Update for OpenShift Container Platform 4.7.9 packages and (RHSA-2021:1366)

[239381](#) Red Hat Update for OpenShift Container Platform 4.7.13 packages and (RHSA-2021:2122)

377556 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0069)
500976 Alpine Linux Security Update for go
501567 Alpine Linux Security Update for go
6140202 AWS Bottlerocket Security Update for golang (GHSA-h382-mj64-43m3)
670942 EulerOS Security Update for golang (EulerOS-SA-2021-1073)
690507 Free Berkeley Software Distribution (FreeBSD) Security Update for go (bc7aff8c-d806-11ea-a5aa-0800272260e5)
770039 Red Hat OpenShift Container Platform 4.6.1 Package Security Update (RHSA-2020:4297)
770040 Red Hat OpenShift Container Platform 4.5.20 Packages and Security Update (RHSA-2020:5119)
770041 Red Hat OpenShift Container Platform 4.6.6 Security Update (RHSA-2020:5159)
770052 Red Hat OpenShift Container Platform 4.5.34 Packages and Security Update (RHSA-2021:0713)
770053 Red Hat OpenShift Container Platform 4.6.23 Security Update (RHSA-2021:0956)
770056 Red Hat OpenShift Container Platform 4.5.37 Security Update (RHSA-2021:1016)
770058 Red Hat OpenShift Container Platform 4.7.9 Packages and Security Update (RHSA-2021:1366)
770063 Red Hat OpenShift Container Platform 4.7.13 Packages and Security Update (RHSA-2021:2122)
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)
770093 Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2021-0713)
770096 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-2122)
770113 Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2021-1016)
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)
900261 CBL-Mariner Linux Security Update for golang 1.13.11
903465 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (1877)
907778 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (1877-1)

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](#)