



# CVE-2020-28367

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-28367
<b>State</b>	PUBLIC
<b>Assigner</b>	security@golang.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-18 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time v

## Risk And Classification

**Problem Types:** CWE-94

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	All	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Insights Telegraf Agent</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Trident</a>	-	All	All	All

## References

Reference	Source	L
cmd/go: improper validation of cgo flags can lead to remote code execution at build time · Issue #42556 · golang/go · GitHub	MISC	<a href="#">g</a>
go.dev/cl/267277	MISC	<a href="#">g</a>
[security] Go 1.15.5 and Go 1.14.12 are released		<a href="#">g</a>
November 2020 Golang Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">s</a>
cmd/go: improper validation of cgo flags can lead to remote code execution at build time · Issue #42556 · golang/go · GitHub	MISC	<a href="#">g</a>

[SECURITY] [DLA 3395-1] golang-1.11 security update	MISC	li
da7aa86917811a571e6634b45a457f918b8e6561 - go - Git at Google		g
[SECURITY] [DLA 2460-1] golang-1.8 security update	MLIST	li
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	s
Pony Mail!	MLIST	li
[SECURITY] Fedora 32 Update: golang-1.14.13-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	li
GO-2022-0476 - Go Packages	MISC	p
[SECURITY] Fedora 33 Update: golang-1.15.5-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	li
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [181743](#) Debian Security Update for golang-1.11 (DLA 3395-1)
- [352291](#) Amazon Linux Security Update for golang: AL2012-2021-332
- [501574](#) Alpine Linux Security Update for go
- [670178](#) EulerOS Security Update for golang (EulerOS-SA-2021-1678)
- [690435](#) Free Berkeley Software Distribution (FreeBSD) Security Update for go (db4b2f27-252a-11eb-865c-00155d646400)
- [710584](#) Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
- [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)
- [900148](#) CBL-Mariner Linux Security Update for golang 1.13.15
- [902887](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3603)
- [907748](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3603-1)
- [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](#)**