



CVE-2020-28366

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

Summary

CVE	CVE-2020-28366
State	PUBLIC
Assigner	security@golang.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	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	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	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	Trident	-	All	All	All

References

Reference	Source	Link	Ta
GO-2022-0475 - Go Packages	MISC	pkg.go.dev	
cmd/go: arbitrary code can be injected into cgo generated files · Issue #42559 · golang/go · GitHub	MISC	github.com	Th
062e0e5ce6df339dc26732438ad771f73dbf2292 - go - Git at Google	MISC	go.googlesource.com	
[security] Go 1.15.5 and Go 1.14.12 are released		groups.google.com	
November 2020 Golang Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
cmd/go: arbitrary code can be injected into cgo generated files · Issue #42559 · golang/go · GitHub		go.dev	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.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	
go.dev/cl/269658		go.dev	
[SECURITY] Fedora 33 Update: golang-1.15.5-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Th
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [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)
- [670947](#) EulerOS Security Update for golang (EulerOS-SA-2021-2582)
- [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
- [903030](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3602)
- [907786](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3602-1)
- [940378](#) AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2020:5493)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report