CVE-2020-28367

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-28367
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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
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	L
cmd/go: improper validation of cgo flags can lead to remote code execution at build time · Issue #42556 · golang/go · GitHub	MISC	g
go.dev/cl/267277	MISC	g
[security] Go 1.15.5 and Go 1.14.12 are released		g
November 2020 Golang Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	s
cmd/go: improper validation of cgo flags can lead to remote code execution at build time · Issue #42556 · golang/go · GitHub	MISC	g

[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	w
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 and Source URL Uptime Status status.cve.report