CVE-2019-11840

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-11840
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-09 16:29:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	An issue was discovered in supplementary Go cryptography libraries, aka golang-googlecode-go-crypto, before 2019-03-20

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Golang	Crypto	All	All	All	All
Application	Golang	Crypto	All	All	All	All

References

Reference
[SECURITY] [DLA 2402-1] golang-go.crypto security update
1691529 – (CVE-2019-11840) CVE-2019-11840 golang-googlecode-go-crypto: Keystream loop in amd64 assembly when overflowing 32-bit c
[SECURITY] [DLA 2527-1] snapd security update
Google Groups
[SECURITY] [DLA 1840-1] golang-go.crypto security update
[SECURITY] [DLA 3455-1] golang-go.crypto security update
[SECURITY] [DLA 2442-1] obfs4proxy security update
[SECURITY] [DLA 2454-1] rclone security update
x/crypto/salsa20: keystream loop in amd64 implementation after 256GiB · Issue #30965 · golang/go · GitHub
Google Groups

b7391e95e576cacdcdd422573063bc057239113d - crypto - Git at Google

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181874 Debian Security Update for golang-go.crypto (DLA 3455-1)