CVE-2020-9283

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-9283
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-20 20:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	golang.org/x/crypto before v0.0.0-20200220183623-bac4c82f6975 for Go allows a panic during signature verification in the

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Golang	Package Ssh	0.0.0-20200220183623-bac4c82f6975	All	All	All
Application	Golang	Package Ssh	0.0.0-20200220183623-bac4c82f6975	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2455-1] packer security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2453-1] restic security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2402-1] golang-go.crypto security update	MLIST	lists.debian.org	
Google Groups	CONFIRM	groups.google.com	Mailing List, Third Party Advisory
Google Groups		groups.google.com	
[SECURITY] [DLA 3455-1] golang-go.crypto security update	MLIST	lists.debian.org	
Go SSH 0.0.2 Denial Of Service ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VDB Ent
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

770028 Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2020:2413)

982579 Go (go) Security Update for golang.org/x/crypto (GHSA-ffhg-7mh4-33c4)