CVE-2023-24532

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-24532
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-08 20:15:00 UTC
Updated	2023-11-07 04:08:00 UTC
Description	The ScalarMult and ScalarBaseMult methods of the P256 Curve may return an incorrect result if called with some specific u

Risk And Classification

Problem Types: CWE-682

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All

References

Reference	Source
crypto/elliptic: specific unreduced P-256 scalars produce incorrect results (CVE-2023-24532) · Issue #58647 · golang/go · GitHub	MISC
GO-2023-1621 - Go Packages	MISC
go.dev/cl/471255	MISC
[security] Go 1.20.2 and Go 1.19.7 are released	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184193 Debian Security Update for golang-1.19 (CVE-2023-24532)

296100 Oracle Solaris 11.4 Support Repository Update (SRU) 58.144.3 Missing (CPUAPR2023)

354890 Amazon Linux Security Advisory for golang : ALAS2-2023-2015

354901 Amazon Linux Security Advisory for golang : ALAS-2023-1731

355216 Amazon Linux Security Advisory for golang : ALAS2023-2023-175

355697 Amazon Linux Security Advisory for golang : ALAS2-2023-2163

355797 Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2023-026

355837 Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2023-029

356180 Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-001

356503 Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001

502862 Alpine Linux Security Update for go

503187 Alpine Linux Security Update for go

506080 Alpine Linux Security Update for go

691086 Free Berkeley Software Distribution (FreeBSD) Security Update for go (742279d6-bdbe-11ed-a179-2b68e9d12706)

753772 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:0733-1)

753839 SUSE Enterprise Linux Security Update for container-suseconnect (SUSE-SU-2023:0871-1)

908039 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (37385-1)