CVE-2017-8932

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-8932
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-06 16:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	A bug in the standard library ScalarMult implementation of curve P-256 for amd64 architectures in Go before 1.7.6 and 1.8.

Risk And Classification

Problem Types: CWE-682

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Application	Golang	Go	1.8	All	All	All
Application	Golang	Go	1.8.1	All	All	All
Application	Golang	Go	1.8	All	All	All
Application	Golang	Go	1.8.1	All	All	All
Application	Golang	Go	All	All	All	All
Application	Novell	Suse Package Hub For Suse Linux Enterprise	12	All	All	All
Application	Novell	Suse Package Hub For Suse Linux Enterprise	12	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All

References

Reference	Source	Link
openSUSE-SU-2017:1650-1: moderate: Security update for go	SUSE	lists.opensuse.org
openSUSE-SU-2017:1649-1: moderate: Security update for go	SUSE	lists.opensuse.org
Google Groups	MLIST	groups.google.com

crypto/elliptic: carry bug in x86-64 P-256 · Issue #20040 · golang/go · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	access.redhat.com
crypto/elliptic: fix carry bug in x86-64 P-256 implementation. · golang/go@9294fa2 · GitHub	CONFIRM	github.com
1455191 – CVE-2017-8932 golang: Elliptic curvers carry propagation issue in x86-64 P-256 [fedora-all]	MISC	bugzilla.redhat.com
[SECURITY] Fedora 25 Update: golang-1.7.6-1.fc25 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 25 Update: golang-1.7.6-1.fc25 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
go-review.googlesource.com/c/41070	CONFIRM	go-review.googlesourc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.