CVE-2019-6486

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-6486
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-24 05:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	Go before 1.10.8 and 1.11.x before 1.11.5 mishandles P-521 and P-384 elliptic curves, which allows attackers to cause a d

Risk And Classification

Problem Types: CWE-770

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
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Golang	Go	All	All	All	All
Application	Golang	Go	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2019:1444-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] [DLA 1664-1] golang security update	MLIST	lists.debian.org
crypto/elliptic: CPU DoS vulnerability affecting P-521 and P-384 · Issue #29903 · golang/go · GitHub	CONFIRM	github.com
[release-branch.go1.11-security] crypto/elliptic: reduce subtraction … · golang/go@42b42f7 · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4379-1 golang-1.7	DEBIAN	www.debian.org
Debian -- Security Information -- DSA-4380-1 golang-1.8	DEBIAN	www.debian.org

[security-announce] openSUSE-SU-2019:1499-1: important: Security update	SUSE	lists.opensuse.org
Google Groups		groups.google.com
[security-announce] openSUSE-SU-2019:1506-1: important: Security update	SUSE	lists.opensuse.org
Google Groups	CONFIRM	groups.google.com
[security-announce] openSUSE-SU-2019:1164-1: moderate: Security update f	SUSE	lists.opensuse.org
GitHub - google/wycheproof: Project Wycheproof tests crypto libraries against known attacks.	MISC	github.com
Golang Go CVE-2019-6486 Remote Denial of Service Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296092 Oracle Solaris 11.4 Support Repository Update (SRU) 7.1.4 Missing (CPUJAN2019)

377556 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0069)

500972 Alpine Linux Security Update for go