CVE-2018-16875

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16875
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-14 14:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	The crypto/x509 package of Go before 1.10.6 and 1.11.x before 1.11.3 does not limit the amount of work performed for eac

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Application	Golang	Go	All	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2019:1444-1: important: Security update	SUSE
Google Groups	
Google Groups	MISC
[security-announce] openSUSE-SU-2019:1079-1: important: Security update	SUSE
[security-announce] openSUSE-SU-2019:1499-1: important: Security update	SUSE
1657565 – (CVE-2018-16875) CVE-2018-16875 golang: crypto/x509 allows for denial of service via crafted TLS client certificate	CONFIRM
[security-announce] openSUSE-SU-2019:1506-1: important: Security update	SUSE
[security-announce] openSUSE-SU-2019:1703-1: moderate: Security update f	SUSE
Go: Multiple vulnerabilities (GLSA 201812-09) — Gentoo security	GENTOO
Golang Go CVE-2018-16875 Remote Denial of Service Vulnerability	BID

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 174971 SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1458-1)
- 296075 Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
- 710317 Gentoo Linux Go Multiple Vulnerabilities (GLSA 201812-09)