CVE-2017-5336

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5336
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-24 15:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x b

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	3.5.0	All	All	All
Application	Gnu	Gnutls	3.5.1	All	All	All
Application	Gnu	Gnutls	3.5.2	All	All	All
Application	Gnu	Gnutls	3.5.3	All	All	All
Application	Gnu	Gnutls	3.5.4	All	All	All
Application	Gnu	Gnutls	3.5.5	All	All	All
Application	Gnu	Gnutls	3.5.6	All	All	All
Application	Gnu	Gnutls	3.5.7	All	All	All
Application	Gnu	Gnutls	3.5.0	All	All	All
Application	Gnu	Gnutls	3.5.1	All	All	All
Application	Gnu	Gnutls	3.5.2	All	All	All
Application	Gnu	Gnutls	3.5.3	All	All	All
Application	Gnu	Gnutls	3.5.4	All	All	All
Application	Gnu	Gnutls	3.5.5	All	All	All
Application	Gnu	Gnutls	3.5.6	All	All	All
Application	Gnu	Gnutls	3.5.7	All	All	All
Application	Gnu	Gnutls	All	All	All	All

Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2017:0386-1: important: Security update	SUSE
GnuTLS	CONFIRM
oss-security - Re: CVE request: two advisories for GnuTLS GNUTLS-SA-2017-1, GNUTLS-SA-2017-2, fixed in 3.3.26, 3.5.8	MLIST
GnuTLS CVE-2017-5336 Stack Buffer Overflow Vulnerability	BID
340 - gnutls: Stack-buffer-overflow in cdk_pk_get_keyid - oss-fuzz - Monorail	MISC
GnuTLS Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTRACK
Red Hat Customer Portal	REDHAT
GnuTLS: Multiple vulnerabilities (GLSA 201702-04) — Gentoo Security	GENTOO
Red Hat Customer Portal	REDHAT
opencdk: cdk_pk_get_keyid: fix stack overflow (5140422e) · Commits · gnutls / GnuTLS · GitLab	CONFIRM
oss-security - CVE request: two advisories for GnuTLS GNUTLS-SA-2017-1, GNUTLS-SA-2017-2, fixed in 3.3.26, 3.5.8	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710395 Gentoo Linux Gnu Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 201702-04)