CVE-2017-5337

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

Summary

CVE	CVE-2017-5337
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	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow re

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
346 - gnutls: Heap-buffer-overflow in _cdk_buftou32 - oss-fuzz - Monorail	MISC
[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 Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTRACK
opencdk: read_attribute: added more precise checks when reading stream (94fcf164) · Commits · gnutls / GnuTLS · GitLab	CONFIRM
Red Hat Customer Portal	REDHAT
GnuTLS: Multiple vulnerabilities (GLSA 201702-04) — Gentoo Security	GENTOO
Red Hat Customer Portal	REDHAT
338 - gnutls: Heap-buffer-overflow in read_attribute - oss-fuzz - Monorail	MISC
GnuTLS 'lib/opencdk/read-packet.c' Multiple Heap Buffer Overflow Vulnerabilities	BID
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)