CVE-2015-3622

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-12 19:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.5 allows remote attackers to cause a deni

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Application	Gnu	Libtasn1	All	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference	Source	Link
USN-2604-1: Libtasn1 vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
GNU Libtasn1 4.5 released	MLIST	lists.gnu.org
[SECURITY] Fedora 21 Update: libtasn1-4.5-1.fc21	FEDORA	lists.fedoraprojec
openSUSE-SU-2016:1674-1: moderate: Security update for libtasn1	SUSE	lists.opensuse.or
GNU Libtasn1 'decoding.c' Heap Buffer Overflow Vulnerability	BID	www.securityfocu
Support / Security / Advisories / / MDVSA-2015:232 | Mandriva	MANDRIVA	www.mandriva.c
Full Disclosure: Heap overflow / invalid read in Libtasn1 before 4.5 (TFPA 005/2015)	FULLDISC	seclists.org
openSUSE-SU-2015:1372-1: moderate: Security update for gnutls	SUSE	lists.opensuse.or
openSUSE-SU-2016:1567-1: moderate: Security update for libtasn1	SUSE	lists.opensuse.or

libtasn1 Heap Overflow ≈ Packet Storm	MISC	packetstormsecu
Red Hat Customer Portal	REDHAT	access.redhat.co
Debian -- Security Information -- DSA-3256-1 libtasn1-6	DEBIAN	www.debian.org
libtASN1 Heap Over-read in _asn1_extract_der_octet() Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytrac
Gentoo Security	GENTOO	security.gentoo.o
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.