CVE-2015-7673

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

Summary

CVE	CVE-2015-7673
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-26 17:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	io-tga.c in gdk-pixbuf before 2.32.0 uses heap memory after its allocation failed, which allows remote attackers to cause a c

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Gdk-pixbuf	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
gdk-pixbuf Heap Buffer Overflow and Denial of Service Vulnerabilities	BID	www.secu
Debian -- Security Information -- DSA-3378-1 gdk-pixbuf	DEBIAN	www.debi
oss-security - Re: CVE request: Heap overflow and DoS with a tga file in gdk-pixbuf < 2.32.1	MLIST	www.oper
gdk-pixbuf: Multiple Vulnerabilities (GLSA 201512-05) — Gentoo Security	GENTOO	security.g
ftp.gnome.org/pub/gnome/sources/gdk-pixbuf/2.32/gdk-pixbuf-2.32.0.news	CONFIRM	ftp.gnome
tga: Wrap TGAColormap struct in its own API (edf6fb8d) · Commits · GNOME / gdk-pixbuf · GitLab	CONFIRM	git.gnome
USN-2767-1: GDK-PixBuf vulnerabilities | Ubuntu	UBUNTU	www.ubur
oss-security - CVE request: Heap overflow and DoS with a tga file in gdk-pixbuf < 2.32.1	MLIST	www.oper
openSUSE-SU-2016:0897-1: moderate: Security update for gdk-pixbuf	SUSE	lists.opens
openSUSE-SU-2016:1467-1: moderate: Security update for gdk-pixbuf	SUSE	lists.opens
pixops: Fail make_weights functions on OOM (19f9685d) · Commits · GNOME / gdk-pixbuf · GitLab	CONFIRM	git.gnome

io-tga: Colormaps are always present, so always parse them. (6ddca835) · Commits · GNOME / gdk-pixbuf · GitLab	CONFIRM	git.gnome
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.