CVE-2017-17682

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

Summary

CVE	CVE-2017-17682
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-14 06:29:00 UTC
Updated	2020-09-08 00:15:00 UTC
Description	In ImageMagick 7.0.7-12 Q16, a large loop vulnerability was found in the function ExtractPostscript in coders/wpg.c, which

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-12	q16	All	All
Application	Imagemagick	Imagemagick	7.0.7-12	q16	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 1227-1] imagemagick security update	MLIST	lists.debian.org	Mailing List,
[SECURITY] [DLA 2366-1] imagemagick security update	MLIST	lists.debian.org	

USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party A
[SECURITY] [DLA 1785-1] imagemagick security update	MLIST	lists.debian.org	
cpu exhaustion in ReadWPGImage · Issue #870 · ImageMagick/ImageMagick · GitHub	CONFIRM	github.com	Exploit, Third
ImageMagick CVE-2017-17682 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**