CVE-2018-5248

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

Summary

CVE	CVE-2018-5248
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-05 19:29:00 UTC
Updated	2019-03-12 15:35:00 UTC
Description	In ImageMagick 7.0.7-17 Q16, there is a heap-based buffer over-read in coders/sixel.c in the ReadSIXELImage function, re

Risk And Classification

Problem Types: CWE-125

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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-17	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-17	All	All	All

References

Reference	Source	Link	Tags

heap-buffer-overflow in sixel_decode · Issue #927 · ImageMagick/ImageMagick · GitHub	CONFIRM	github.com	Exploit, Thi
Malformed Request	BID	www.securityfocus.com	Third Party
USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party
Debian -- Security Information -- DSA-4245-1 imagemagick	DEBIAN	www.debian.org	Third Party
Debian -- Security Information -- DSA-4204-1 imagemagick	DEBIAN	www.debian.org	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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**