CVE-2018-18025

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-18025
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-07 18:29:00 UTC
Updated	2020-09-08 00:15:00 UTC
Description	In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the EncodeImage function of coders/pict.c, which a

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Imagemagick	Imagemagick	7.0.8-13	q16	All	All
Application	Imagemagick	Imagemagick	7.0.8-13	q16	All	All

References

Reference	Source	Link	Tags
heap-buffer-overflow in EncodeImage of pict.c · Issue #1335 · ImageMagick/ImageMagick · GitHub	MISC	github.com	Exploit,
[SECURITY] [DLA 1574-1] imagemagick security update	MLIST	lists.debian.org	Mailing l
[SECURITY] [DLA 2366-1] imagemagick security update	MLIST	lists.debian.org	
USN-4034-1: ImageMagick vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501010 Alpine Linux Security Update for imagemagick6

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