CVE-2018-18023

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-18023
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-07 18:29:00 UTC
Updated	2019-06-25 15:15:00 UTC
Description	In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the SVGStripString function of coders/svg.c, which

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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 SVGStripString of svg.c · Issue #1336 · ImageMagick/ImageMagick · GitHub	MISC	github.com	Exploit
USN-4034-1: ImageMagick vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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

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