CVE-2023-3745

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

Summary

CVE	CVE-2023-3745
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-24 16:15:00 UTC
Updated	2023-11-07 04:19:00 UTC
Description	A heap-based buffer overflow issue was found in ImageMagick's PushCharPixel() function in quantum-private.h. This issue

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	All	All	All	All

References

Reference	Source	Lin
https://github.com/ImageMagick/ImageMagick/issues/1857 · ImageMagick/ImageMagick@54cdc14 · GitHub	MISC	gith
https://github.com/ImageMagick/ImageMagick/issues/1857 · ImageMagick/ImageMagick@651672f · GitHub	MISC	gith
cve-details	MISC	acc
2223557 – (CVE-2023-3745) CVE-2023-3745 ImageMagick: heap-buffer-overflow in PushCharPixel() in quantum-private.h	MISC	bug
https://github.com/ImageMagick/ImageMagick/issues/1857 · ImageMagick/ImageMagick6@7486477 · GitHub	MISC	gith
heap-buffer-overflow in /MagickCore/quantum-private.h · Issue #1857 · ImageMagick/ImageMagick · GitHub	MISC	gith
https://github.com/ImageMagick/ImageMagick/issues/1857 · ImageMagick/ImageMagick6@b466a96 · GitHub	MISC	gith
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

355755 Amazon Linux Security Advisory for ImageMagick : ALAS-2023-1791

355787 Amazon Linux Security Advisory for ImageMagick : ALAS2-2023-2178

754285 SUSE Enterprise Linux Security Update for ImageMagick (SUSE-SU-2023:3357-1)