CVE-2023-34475

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

Summary

CVE	CVE-2023-34475
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-16 20:15:00 UTC
Updated	2023-11-07 04:15:00 UTC
Description	A heap use after free issue was discovered in ImageMagick's ReplaceXmpValue() function in MagickCore/profile.c. An atta

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All

References

Reference
[SECURITY] Fedora 37 Update: ImageMagick-6.9.12.93-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 38 Update: ImageMagick-7.1.1.15-1.fc38 - package-announce - Fedora Mailing-Lists
2214149 – (CVE-2023-34475) CVE-2023-34475 ImageMagick: heap use-after-free issue in ReplaceXmpValue() function in MagickCore/profile
[SECURITY] Fedora 37 Update: ImageMagick-6.9.12.93-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 38 Update: ImageMagick-7.1.1.15-1.fc38 - package-announce - Fedora Mailing-Lists
cve-details
carefully crafted image files (TIM2, JPEG) no longer overflow buffer … · ImageMagick/ImageMagick@1061db7 · GitHub
CVE Program record
NVD vulnerability detail

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**