



CVE-2020-25663

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-25663
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-08 21:15:00 UTC
Updated	2021-06-02 19:43:00 UTC
Description	A call to ConformPixelInfo() in the SetImageAlphaChannel() routine of /MagickCore/channel.c caused a subsequent heap-u

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

1891601 – (CVE-2020-25663) CVE-2020-25663 ImageMagick: use-after-free, heap-buffer-overflow triggered by GetPixelRed, GetPixelBlue in heap-use-after-free at MagickCore/pixel-accessor.h in GetPixelRed · Issue #1723 · ImageMagick/ImageMagick · GitHub

heap-use-after-free at MagickCore/pixel-accessor.h in GetPixelRed · Issue #1723 · ImageMagick/ImageMagick · 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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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