



CVE-2020-25674

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-25674
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-08 22:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	WriteOnePNGImage() from coders/png.c (the PNG coder) has a for loop with an improper exit condition that can allow an o

Risk And Classification

Problem Types: CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All

References

Reference	Source
1891928 – (CVE-2020-25674) CVE-2020-25674 ImageMagick: heap-based buffer overflow in WriteOnePNGImage in coders/png.c	MISC
[SECURITY] [DLA 2523-1] imagemagick security update	MLIST
[SECURITY] [DLA 3357-1] imagemagick security update	MLIST
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181625](#) Debian Security Update for imagemagick (DLA 3357-1)

198406 Ubuntu Security Notification for ImageMagick vulnerabilities (USN-4988-1)
671560 EulerOS Security Update for ImageMagick (EulerOS-SA-2022-1536)
671612 EulerOS Security Update for ImageMagick (EulerOS-SA-2022-1570)
671705 EulerOS Security Update for ImageMagick (EulerOS-SA-2022-1731)
750398 OpenSUSE Security Update for ImageMagick (openSUSE-SU-2021:0148-1)
750404 OpenSUSE Security Update for ImageMagick (openSUSE-SU-2021:0136-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)