



CVE-2023-2804

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

Summary

CVE	CVE-2023-2804
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-25 22:15:00 UTC
Updated	2023-08-17 19:26:00 UTC
Description	A heap-based buffer overflow issue was discovered in libjpeg-turbo in h2v2_merged_upsample_internal() function of jdmg...

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libjpeg-turbo	Libjpeg-turbo	All	All	All	All
Application	Libjpeg-turbo	Libjpeg-turbo	2.1.90	All	All	All

References

Reference

- Heap Buffer Overflow in /libjpeg-turbo/jquant2.c:224 at prescan_quantize() (SIGSEGV) · Issue #668 · libjpeg-turbo/libjpeg-turbo · GitHub
- cve-details
- heap-buffer-overflow at /libjpeg-turbo/jdmgext.c:126 in h2v2_merged_upsample_internal() (SIGSEGV) · Issue #675 · libjpeg-turbo/libjpeg-turbo
- Lossless decomp: Range-limit 12-bit samples · libjpeg-turbo/libjpeg-turbo@9f756bc · GitHub
- 2208447 – (CVE-2023-2804) CVE-2023-2804 libjpeg-turbo: heap-buffer-overflow in h2v2_merged_upsample_internal() at /libjpeg-turbo/jdmg...
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

503114 Alpine Linux Security Update for libjpeg-turbo

© [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](#).

Free CVE JSON API [cve.report/api](#)

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