



CVE-2023-40889

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

Summary

CVE	CVE-2023-40889
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-29 17:15:00 UTC
Updated	2023-12-01 12:15:00 UTC
Description	A heap-based buffer overflow exists in the qr_reader_match_centers function of ZBar 0.23.90. Specially crafted QR codes i

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zbar Project	Zbar	0.23.90	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3675-1] zbar security update		lists.debian.org	
ZBar Heap-based Buffer Overflow Vulnerability - HackMD		hackmd.io	
ZBar Heap-based Buffer Overflow Vulnerability - HackMD	MISC	hackmd.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284865](#) Fedora Security Update for zbar (FEDORA-2024-583e4098b9)

[285056](#) Fedora Security Update for zbar (FEDORA-2024-73d5220ed3)

[356743](#) Amazon Linux Security Advisory for zbar : ALAS-2023-1887

[506291](#) Alpine Linux Security Update for zbar

6000367	Debian Security Update for zbar (DLA 3675-1)
6000468	Debian Security Update for zbar (DSA 5614-1)
755529	SUSE Enterprise Linux Security Update for zbar (SUSE-SU-2023:4948-1)

© [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](#).

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

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