



CVE-2022-44840

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

Summary

CVE	CVE-2022-44840
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-22 19:16:00 UTC
Updated	2023-08-26 02:14:00 UTC
Description	Heap buffer overflow vulnerability in binutils readelf before 2.40 via function find_section_in_set in file readelf.c.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Binutils	All	All	All	All

References

Reference	Source	Link	Tags
29732 – A heap buffer overflow was found in find_section_in_set() of binutils-2.39 (commit 49c843e6)	MISC	sourceware.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199762](#) Ubuntu Security Notification for GNU binutils Vulnerabilities (USN-6381-1)

[200044](#) Ubuntu Security Notification for GNU binutils Vulnerabilities (USN-6581-1)

[673433](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3001)

[673568](#) EulerOS Security Update for binutils (EulerOS-SA-2024-1331)

[673613](#) EulerOS Security Update for binutils (EulerOS-SA-2023-3024)

673757 EulerOS Security Update for binutils (EulerOS-SA-2024-1309)

674122 EulerOS Security Update for binutils (EulerOS-SA-2024-1503)

674153 EulerOS Security Update for binutils (EulerOS-SA-2024-1482)

754877 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2023:3695-1)

754965 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2023:3825-1)

© [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](#)