



CVE-2017-17122

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

Summary

CVE	CVE-2017-17122
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-04 08:29:00 UTC
Updated	2023-11-07 02:41:00 UTC
Description	The dump_relocs_in_section function in objdump.c in GNU Binutils 2.29.1 does not check for reloc count integer overflows,

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Binutils	2.29.1	All	All	All
Application	Gnu	Binutils	2.29.1	All	All	All

References

Reference	Source	Link	Tags
Binutils: Multiple vulnerabilities (GLSA 201811-17) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
sourceware.org Git - binutils-gdb.git/commit		sourceware.org	
22508 – Heap overflow in dump_relocs_in_section	MISC	sourceware.org	Exploit, Issue Tracking, Patch, This affects
sourceware.org Git - binutils-gdb.git/commit	MISC	sourceware.org	Patch
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

[199808](#) Ubuntu Security Notification for GNU binutils Vulnerabilities (USN-6413-1)

[710297](#) Gentoo Linux Binutils Multiple Vulnerabilities (GLSA 201811-17)

© [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](#)