



CVE-2017-16830

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

Summary

CVE	CVE-2017-16830
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-15 08:29:00 UTC
Updated	2023-11-07 02:40:00 UTC
Description	The print_gnu_property_note function in readelf.c in GNU Binutils 2.29.1 does not have integer-overflow protection on 32-bit

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	
22384 – heap buffer overflow in print_gnu_property_note	CONFIRM	sourceware.org	Exploit, Issue Tracking, Patch
GNU Binutils 'readelf.c' Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Ent
sourceware.org Git - binutils-gdb.git/commit	CONFIRM	sourceware.org	Patch
sourceware.org Git - binutils-gdb.git/commit		sourceware.org	
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

[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](#)