



CVE-2017-6965

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

Summary

CVE	CVE-2017-6965
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-17 09:59:00 UTC
Updated	2017-09-19 01:36:00 UTC
Description	readelf in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-difference relc

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Binutils	2.28	All	All	All
Application	Gnu	Binutils	2.28	All	All	All

References

Reference	Source	Link	Tags
Binutils: Multiple vulnerabilities (GLSA 201709-02) — Gentoo security	GENTOO	security.gentoo.org	
21137 – readelf - heap buffer overflow in elfcomm	CONFIRM	sourceware.org	Exploit, Issue Tracking
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.

There are currently no legacy QID mappings associated with this CVE.

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