



# CVE-2017-6969

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-6969                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2017-03-17 09:59:00 UTC                                                                                                     |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC                                                                                                     |
| <b>Description</b>     | readelf in GNU Binutils 2.28 is vulnerable to a heap-based buffer over-read while processing corrupt RL78 binaries. The vul |

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product                  | Version | Update | Edition | Language |
|-------------|---------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Gnu</a> | <a href="#">Binutils</a> | 2.28    | All    | All     | All      |
| Application | <a href="#">Gnu</a> | <a href="#">Binutils</a> | 2.28    | All    | All     | All      |

## References

| Reference                                                             | Source  | Link                                                              | Tags                             |
|-----------------------------------------------------------------------|---------|-------------------------------------------------------------------|----------------------------------|
| Binutils: Multiple vulnerabilities (GLSA 201709-02) — Gentoo security | GENTOO  | <a href="https://security.gentoo.org">security.gentoo.org</a>     |                                  |
| GNU BinUtils CVE-2017-6969 Remote Denial of Service Vulnerability     | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a> |                                  |
| 21156 – readelf segfault - invalid read of size 4                     | CONFIRM | <a href="https://sourceware.org">sourceware.org</a>               | Exploit, Issue Tracking, Third I |
| CVE Program record                                                    | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical                        |
| NVD vulnerability detail                                              | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis              |

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)