



# CVE-2017-14529

Published on: 09/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

## CVE-2017-14529

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Binutils](#) from [Gnu](#) contain the following vulnerability:

The `pe_print_idata` function in `peXXigen.c` in the Binary File Descriptor (BFD) library (aka `libbfd`), as distributed in GNU Binutils 2.29, mishandles `HintName` vector entries, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PE file, related to the `bfd_getl16` function.

CVE-2017-14529 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                  | Tags                                                                                                                                                           | Link                                                                  |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 22113 – Heap out of bounds read in <code>bfd_getl16()</code> | <a href="#">Issue Tracking</a><br><a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">sourceware.org</a><br><a href="#">text/html</a> | <a href="#">CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=22113</a> |

sourceware.org Git - binutils-gdb.git/commit

Issue Tracking

Patch

Third Party Advisory

sourceware.org

text/xml

CONFIRM

sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=dcaaca89e8618eba35193c27afc1cfa54f74582

sourceware.org Git - binutils-gdb.git/commit

Issue Tracking

Patch

Third Party Advisory

sourceware.org

text/xml

CONFIRM

sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=4d465c689a8fb27212ef358d0aee89d60dee69a6

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type        | Vendor | Product  | Version | Update | Edition | Language |
|-------------|--------|----------|---------|--------|---------|----------|
| Application | Gnu    | Binutils | 2.29    | All    | All     | All      |
| Application | Gnu    | Binutils | 2.29    | All    | All     | All      |

cpe:2.3:a:gnu:binutils:2.29:\*:\*:\*:\*:\*:

cpe:2.3:a:gnu:binutils:2.29:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →