



CVE-2017-15020

Published on: 10/04/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:39:00 AM UTC

CVE-2017-15020

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

Certain versions of [Binutils](#) from [Gnu](#) contain the following vulnerability: dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles pointers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, related to parse_die and parse_line_table, as demonstrated by a parse_die heap-based buffer over-read.

CVE-2017-15020 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
sourceware.org Git - binutils-gdb.git/commit	sourceware.org text/xml	MISC sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=1da5c9a485f3dcac4c45e96ef4b7dae5948314b5
22202 - heap-based buffer overflow in parse_die	Issue Tracking	MISC sourceware.org/bugzilla/show_bug.cgi?id=22202

22202 heap-based buffer overflow in parse_die (dwarf1.c)

Issue Tracking

Patch

Third Party Advisory

sourceware.org

text/html

INFO

sourceware.org/bugzilla/show_bug.cgi?id=22202

binutils: heap-based buffer overflow in parse_die (dwarf1.c) | agostino's blog

Patch

Third Party Advisory

VDB Entry

blogs.gentoo.org

text/html

MISC

blogs.gentoo.org/ago/2017/10/03/binutils-heap-based-buffer-overflow-in-parse_die-dwarf1-c/

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.

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