



CVE-2017-15022

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

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

CVE-2017-15022

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

Certain versions of [Binutils](#) from [Gnu](#) contain the following vulnerability: dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the DW_AT_name data type, which allows remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds access, and application crash) via a crafted ELF file, related to scan_unit_for_symbols and parse_comp_unit.

CVE-2017-15022 has been assigned by [M](#) 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
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
22201 – DW_AT_name with out of bounds reference	Issue Tracking Patch Third Party Advisory	MISC sourceware.org/bugzilla/show_bug.cgi?id=22201

sourceware.org

text/html

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

sourceware.org

text/xml

MISC

sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=11855d8a1f11b102a702ab76e95b22082cccf2f8

binutils: NULL pointer dereference in bfd_hash_hash (hash.c) | agostino's blog

Patch

Third Party Advisory

VDB Entry

blogs.gentoo.org

text/html

MISC

blogs.gentoo.org/ago/2017/10/03/binutils-null-pointer-dereference-in-bfd_hash_hash-hash-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

← Previous ID

Next ID →