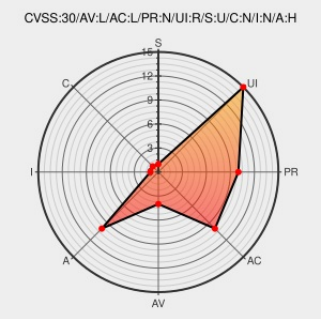
CVE-2017-15021

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

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

CVE-2017-15021

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Binutils from Gnu contain the following vulnerability:

bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_getl32.

CVE-2017-15021 has been assigned by 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
binutils: heap-based buffer overflow in bfd_get_debug_link_info_1 (opncls.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-bfd_getl32-opncls-c/

sourceware.org Git - binutils-gdb.git/commit	sourceware.org text/xml	MISC sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=52b36c51e5bf6d7600fdc6ba115b170b0e78e31d
22197 – buffer overflow in bfd_get_debug_link_info_1	Issue Tracking Patch Third Party Advisory sourceware.org text/html	MISC sourceware.org/bugzilla/show_bug.cgi?id=22197

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→