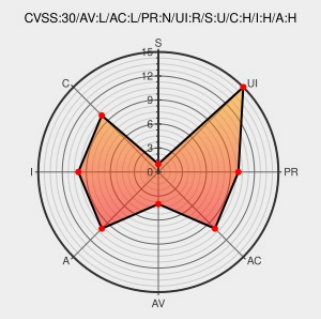
CVE-2017-14745

Published on: 09/26/2017 12:00:00 AM UTC

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

CVE-2017-14745

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



Certain versions of Binutils from Gnu contain the following vulnerability:

The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, interpret a -1 value as a sorting count instead of an error flag, which allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.

CVE-2017-14745 has been assigned by 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
22148 – Integer overflow in elf64-x86-64.c, binutils 2.29.1	Issue Tracking Patch Third Party Advisory	CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=22148

sourceware.org
text/html

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→