

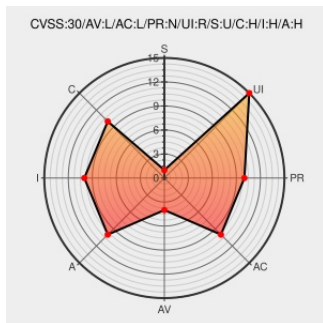


CVE-2017-12448

Published on: 08/04/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-12448

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

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

The `bfd_cache_close` function in `bfd/cache.c` in the Binary File Descriptor (BFD) library (aka `libbfd`), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the `bfd_generic_archive_p` function in `bfd/archive.c`.

CVE-2017-12448 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
21787 – Heap-use-after-free in <code>bfd_cache_close</code>	Issue Tracking Patch	MISC sourceware.org/bugzilla/show_bug.cgi?id=21787

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	All	All	All	All
cpe:2.3:a:gnu:binutils:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)