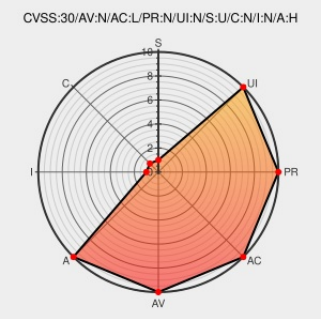
CVE-2017-8396

Published on: 05/01/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-8396

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



Certain versions of Binutils from Gnu contain the following vulnerability:

The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read of size 1 because the existing reloc offset range tests didn't catch small negative offsets less than the size of the reloc field. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objdump, to crash.

CVE-2017-8396 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Binutils: Multiple vulnerabilities (GLSA 201709-02) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201709-02
21432 – heap buffer overflow in objdump	Issue Tracking	CONFIRM sourceware.org/bugzilla/show_bug.cgi?

21432 - heap buffer overflow in objdump

Issue Tracking
Patch
Third Party Advisory
sourceware.org
text/html

https://sourceware.org/bugzilla/show_bug.cgi?id=21432

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	2.28	All	All	All
Application	Gnu	Binutils	2.28	All	All	All

cpe:2.3:a:gnu:binutils:2.28:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:binutils:2.28:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→