

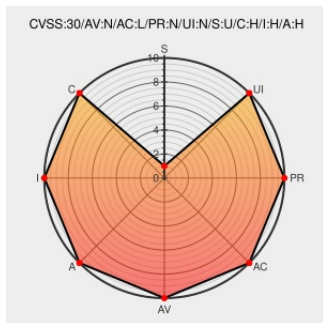


CVE-2017-7614

Published on: 04/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:40 PM UTC

CVE-2017-7614

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

Certain versions of [Binutils](#) from [Gnu](#) contain the following vulnerability: elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a "member access within null pointer" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an "int main() {return 0;}" program.

CVE-2017-7614 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
binutils: two NULL pointer dereference in elflink.c agostino's blog	Exploit Patch Third Party Advisory blogs.gentoo.org text/html	MISC blogs.gentoo.org/ago/2017/04/05/binutils-two-null-pointer-dereference-in-elflink-c/

Related QID Numbers

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE