



## Bug 2443828 (CVE-2026-3442) - CVE-2026-3442 binutils: GNU Binutils: Information disclosure or denial of service via out-of-bounds read in bfd linker

**Keywords:** Security

**Reported:** 2026-03-02 14:16 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-03-02 14:43 UTC ([History](#))

**Alias:** CVE-2026-3442

**CC List:** 7 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**


**Whiteboard:**

**Depends On:** [2443830](#) [2443831](#) [2443832](#)  
[2443835](#) [2443836](#) [2443837](#)  
[2443833](#) [2443834](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport  2026-03-02 14:16:00 UTC[Description](#)

Summary: A separate heap-based buffer overflow (Out-of-Bounds Read) was found in GNU Binutils (bfd linker) in bfd/xcofflink.c. This issue occurs in xcoff\_link\_add\_symbols (approx line 2282) where r\_symndx is used to index symbol hashes without sufficient bounds checking.  
Requirements to exploit: An attacker needs to trick a user into running the ld linker against a specially crafted malicious XCOFF object file.

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

