Bug 2443826 (CVE-2026-3441) - CVE-2026-3441 binutils: GNU Binutils: Information disclosure via specially crafted XCOFF object file

Keywords: Security

Status: NEW

Alias: CVE-2026-3441

Product: Security Response

Component: vulnerability

Version: unspecified

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

Reported: 2026-03-02 14:08 UTC by OSIDB Bzimport

Modified: 2026-03-02 14:43 UTC (History)

CC List: 7 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-02 14:08:14 UTC Description

```
Summary: A heap-based buffer overflow (Out-of-Bounds Read) was
found in GNU Binutils (bfd linker). The vulnerability occurs
in bfd/xcofflink.c in the xcoff_link_add_symbols function. It
is caused by an improper check of the x_scnlen value, leading
to an out-of-bounds access on the csects array.
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.