Bug 1911691 (CVE-2020-35507) - CVE-2020-35507 binutils: NULL pointer dereference in bfd_pef_parse_function_stubs function in bfd/pef.c

Keywords: Security ×

Status: NEW

Alias: CVE-2020-35507

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~1911694~~ 1911719 1911720 1911721 1911722 1912337 1912338 1912339 1912340 1912341 1912343 1912344 1912345 1912346 1912347 1912348 1912349 1912350 1912351 1912352 1912353 1912354 1912355 1912356 1912357 1912358 1912359 1912360 1912361 1912362 1912363 1912364 1912365 1912366 1912367 1912368 1912369 1912370 1912371 1912372 1912373 1912374 1912375

Blocks: 1908372 1911446

TreeView+ depends on / blocked

Reported: 2020-12-30 17:15 UTC by Guilherme de Almeida Suckevicz

Modified: 2021-11-14 22:29 UTC (History)

CC List: 23 users (show)

Fixed In Version: binutils 2.34

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in bfd_pef_parse_function_stubs of bfd/pef.c in binutils which could allow an attacker who is able to submit a crafted file to be processed by objdump to cause a NULL pointer dereference. The greatest threat of this flaw is to application availability.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Guilherme de Almeida Suckevicz 2020-12-30 17:15:17 UTC — Description

GNU Binutils before 2.34 has a NULL pointer dereference in bfd_pef_parse_function_stubs function in bfd/pef.c due to not checking return value of bfd_malloc.
This bug allows attackers to cause a denial of service.

Reference:
https://sourceware.org/bugzilla/show_bug.cgi?id=25308

Guilherme de Almeida Suckevicz 2020-12-30 17:39:43 UTC — Comment 1

Created mingw-binutils tracking bugs for this issue:

Affects: fedora-all [~~Bug 1911694~~]

Todd Cullum 2020-12-30 20:38:15 UTC — Comment 3

Statement:

binutils as shipped with Red Hat Enterprise Linux 8's GCC Toolset 10 and Red Hat Developer Toolset 10 are not affected by this flaw because the versions shipped have already received the patch.

Todd Cullum 2020-12-30 20:40:30 UTC — Comment 4

Flaw technical summary:

The `bfd_pef_parse_function_stubs()` function in bfd/pef.c allocates memory with `bfd_malloc()` and doesn't check for NULL before passing the returned pointer to `bfd_read()` which dereferences it. An attacker who could submit a crafted input file that makes `bfd_malloc()` fail could cause a denial of service. The upstream patch addresses the issue by adding a NULL check before calling `bfd_read()`.

Todd Cullum 2020-12-30 20:42:33 UTC — Comment 5

Upstream commit: https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=7a0fb7be96e0ce79e1ae429bc1ba913e5244d537

Note
You need to log in before you can comment on or make changes to this bug.