Bug 1911444 (CVE-2020-35496) - CVE-2020-35496 binutils: NULL pointer dereference in bfd_pef_scan_start_address function in bfd/pef.c

Keywords: Security ×

Status: NEW

Alias: CVE-2020-35496

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: ~~1911445~~ 1911711 1911712 1911713 1911714

Blocks: 1908372 1911446

TreeView+ depends on / blocked

Reported: 2020-12-29 13:39 UTC by Guilherme de Almeida Suckevicz

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

CC List: 19 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_scan_start_address() 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 2020-12-29 13:39:10 UTC — Description

GNU Binutils before 2.34 has a NULL pointer dereference in bfd_pef_scan_start_address 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 2020-12-29 13:39:30 UTC — Comment 1

Created mingw-binutils tracking bugs for this issue:

Affects: fedora-all [~~Bug 1911445~~]

Todd Cullum 2020-12-30 20:26:56 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 20:31:35 UTC — Comment 5

Flaw technical summary:

In the `bfd_pef_scan_start_address()` function in bfd/pef.c, `bfd_malloc()` is called and the return pointer is not checked for point to NULL before it is passed to `bfd_read()` which dereferences it. If an attacker is able to cause `bfd_malloc()` to fail/return NULL, they could cause a denial of service. The upstream patch adds a NULL check before calling `bfd_read()`.

Todd Cullum 2020-12-30 20:41:13 UTC — Comment 6

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.