Bug 1911437 (CVE-2020-35493) - CVE-2020-35493 binutils: heap-based buffer overflow in bfd_pef_parse_function_stubs function in bfd/pef.c via crafted PEF file

Keywords: Security ×

Status: NEW

Alias: CVE-2020-35493

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: ~~1911438~~ 1911507 1911508 1911510 1911511 1912249 1912250 1912251 1912252

Blocks: 1908372 1911446

TreeView+ depends on / blocked

Reported: 2020-12-29 13:21 UTC by Guilherme de Almeida Suckevicz

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

CC List: 22 users (show)

Fixed In Version: binutils 2.34

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in Binutils in bfd/pef.c. This flaw allows an attacker who can submit a crafted PEF file to be parsed by objdump to cause a heap buffer overflow, leading to an out-of-bounds read. The highest threat from this vulnerability is to system availability.

Clone Of:

Environment:

Last Closed:

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

Guilherme de Almeida Suckevicz 2020-12-29 13:21:16 UTC Description

```
Objdump of GNU Binutils before 2.34 has a heap-buffer-overflow in function bfd_pef_parse_function_stubs (file bfd/pef.c) which could allow attackers to cause a
denial of service or unspecified impact.

Reference:
https://sourceware.org/bugzilla/show_bug.cgi?id=25307
```

Guilherme de Almeida Suckevicz 2020-12-29 13:21:34 UTC Comment 1

```
Created mingw-binutils tracking bugs for this issue:

Affects: fedora-all [ ~~Bug 1911438~~ ]
```

Todd Cullum 2020-12-30 00:38:52 UTC Comment 5

```
Flaw technical summary:

This flaw is caused by an improper length check followed by a call to `bfd_pef_parse_function_stub()` in `bfd_pef_parse_function_stubs()` of bfd/pef.c. There's a
length check for `if ((codepos + 4) > codelen)`, but the subsequent call to `bfd_pef_parse_function_stub()` passes in length 24, which could read past the end of
the `codebuf` buffer.
```

Todd Cullum 2020-12-30 20:46:19 UTC Comment 6

```
Upstream commit: https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=f2a3559d54602cecfec6d90f792be4a70ad918ab
```

RaTasha Tillery-Smith 2021-02-22 18:50:20 UTC Comment 11

```
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.
```

Note

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