Bug 1911441 (CVE-2020-35495) - CVE-2020-35495 binutils: NULL pointer dereference in bfd_pef_parse_symbols function in bfd/pef.c

Keywords: Security ×

Status: NEW

Alias: CVE-2020-35495

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: ~~1911442~~ 1911549 1911550 1911551 1911552 1912295 1912296 1912297 1912298 1912300 1912301 1912302 1912303 1912304 1912305 1912306 1912307 1912308 1912309 1912310 1912311 1912312 1912313 1912314 1912315 1912316 1912317 1912318 1912319 1912320 1912321 1912322 1912323 1912324 1912325 1912326 1912327 1912329 1912330 1912331 1912332 1912333 1912334

Blocks: 1908372 1911446

TreeView+ depends on / blocked

Reported: 2020-12-29 13:33 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 binutils. An attacker who is able to submit a crafted input file to be processed by the objdump program could cause a null pointer dereference. The greatest threat from 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 13:33:21 UTC — Description

GNU Binutils before 2.34 has a NULL pointer deference vulnerability in function bfd_pef_parse_symbols (file bfd/pef.c) which could allow attackers to cause a denial of service.

Reference:
https://sourceware.org/bugzilla/show_bug.cgi?id=25306

Guilherme de Almeida Suckevicz 2020-12-29 13:33:44 UTC — Comment 1

Created mingw-binutils tracking bugs for this issue:

Affects: fedora-all [~~bug 1911442~~]

Todd Cullum 2020-12-30 00:45:18 UTC — Comment 2

Flaw technical summary:

In `bfd_pef_parse_symbols()` of bfd/pef.c, a call is made to `bfd_malloc()` and the return pointer is dereferenced and written to in a call to `bfd_bread()` without first checking to ensure that the pointer does not point to NULL. Due to the fact that a crafted file could cause this allocation to fail, it's possible for an attacker to trigger a NULL pointer dereference.

Todd Cullum 2020-12-30 00:52:38 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 20:44:48 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.