Bug 1911439 (CVE-2020-35494) - CVE-2020-35494 binutils: usage of unitialized heap in tic4x_print_cond function in opcodes/tic4x-dis.c

Keywords: Security ×

Status: NEW

Alias: CVE-2020-35494

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: ~~1911440~~ 1911518 1911519 1911520 1911521 1912254 1912255 1912256 1912257 1912258 1912259 1912260 1912261 1912262 1912263 1912264 1912265 1912266 1912267 1912268 1912269 1912270 1912271 1912272 1912273 1912274 1912275 1912276 1912278 1912279 1912280 1912281 1912282 1912283 1912284 1912285 1912286 1912287 1912288 1912289 1912290 1912291 1912292

Blocks: 1908372 1911446

TreeView+ depends on / blocked

Reported: 2020-12-29 13:28 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 binutils could cause usage of uninitialized memory. The highest threat is to application availability with a lower threat to data confidentiality.

Clone Of:

Environment:

Last Closed:

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

Guilherme de Almeida Suckevicz 2020-12-29 13:28:49 UTC — Description

GNU Binutils before 2.34 has an uninitialized-heap vulnerability in function tic4x_print_cond (file opcodes/tic4x-dis.c) which could allow attackers to make an information leak.

Reference:
https://sourceware.org/bugzilla/show_bug.cgi?id=25319

Guilherme de Almeida Suckevicz 2020-12-29 13:29:10 UTC — Comment 1

Created mingw-binutils tracking bugs for this issue:

Affects: fedora-all [~~Bug 1911440~~]

Todd Cullum 2020-12-30 00:15:17 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 00:26:13 UTC — Comment 4

Flaw technical summary:

In routine tic4x_print_cond() of opcodes/tic4x-dis.c, xmalloc() is called to allocate 32 bytes, 20 of which are initialized. It is possible for the uninitialized bytes to be reached in a subsequent call to `(*info->fprintf_func)`. This could cause a crash or print the uninitialized data. The upstream patch addresses this flaw by replacing the call to xmalloc() with xcalloc(), which 0-initializes all of the bytes upon allocation.

Todd Cullum 2020-12-30 20:45:31 UTC — Comment 6

Upstream commit: https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=2c5b6e1a1c406cbe06e2d6f77861764ebd01b9ce

---

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