Bug 1937784 (CVE-2021-20284) - CVE-2021-20284 binutils: Heap-based buffer overflow in _bfd_elf_slurp_secondary_reloc_section in elf.c

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2021-20284
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: ~~1943301~~ 1949308 1961525 1961526
Blocks: 1937793 1937804
TreeView+ depends on / blocked

Reported: 2021-03-11 14:44 UTC by Pedro Sampaio
Modified: 2021-11-09 22:24 UTC (History)
CC List: 22 users (show)
Fixed In Version:
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in GNU Binutils 2.35.1, where there is a heap-based buffer overflow in _bfd_elf_slurp_secondary_reloc_section in elf.c due to the number of symbols not calculated correctly. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-11-09 22:24:01 UTC

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:4364	0	None	None	None	2021-11-09 18:28:44 UTC

Pedro Sampaio 2021-03-11 14:44:33 UTC — Description

A flaw was found in GNU Binutils 2.35.1. There is a heap-based buffer overflow in _bfd_elf_slurp_secondary_reloc_section in elf.c because the number of symbols is not caculated correctly.

Upstream bug:

https://sourceware.org/bugzilla/show_bug.cgi?id=26931

Pedro Sampaio 2021-03-25 18:28:01 UTC — Comment 3

Created binutils tracking bugs for this issue:

Affects: fedora-all [~~bug 1943301~~]

Stefan Cornelius 2021-05-18 07:55:43 UTC — Comment 7

Patch:
https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=f60742b2a1988d276c77d5c1011143f320d9b4cb

errata-xmlrpc 2021-11-09 18:28:41 UTC — Comment 8

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2021:4364 https://access.redhat.com/errata/RHSA-2021:4364

Product Security DevOps Team 2021-11-09 22:23:57 UTC — Comment 9

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2021-20284

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