Bug 2121800 (CVE-2022-2905) - CVE-2022-2905 kernel: slab-out-of-bound read in bpf

Keywords: Security ×

Status: NEW

Alias: CVE-2022-2905

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2121801~~ 🔒 2124624 🔒 2124625 🔒 2124626 🔒 2124627

Blocks: 🔒 2119814 🔒 2119817

TreeView+ depends on / blocked

Reported: 2022-08-26 16:43 UTC by Marian Rehak

Modified: 2022-09-20 14:05 UTC (History)

CC List: 52 users (show)

Fixed In Version: Linux kernel 6.0-rc4

Doc Type: If docs needed, set a value

Doc Text: An out-of-bounds memory read flaw was found in the Linux kernel's BPF subsystem in how a user calls the bpf_tail_call function with a key larger than the max_entries of the map. This flaw allows a local user to gain unauthorized access to data.

Clone Of:

Environment:

Last Closed:

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

Marian Rehak 2022-08-26 16:43:58 UTC Description

A bug in the x86 BPF JIT compiler. A bpf_tail_call with a key larger than the max_entries of the map can cause an out-of-bound access when the x86 JIT compiler tries to index bpf_array->ptr using the invalid key.

References:

https://www.openwall.com/lists/oss-security/2022/08/26/1
https://lore.kernel.org/bpf/984b37f9fdf7ac36831d2137415a4a915744c1b6.1661462653.git.daniel@iogearbox.net/

Marian Rehak 2022-08-26 16:44:31 UTC Comment 1

Created kernel tracking bugs for this issue:

Affects: fedora-all [~~bug 2121801~~]

Justin M. Forbes 2022-09-20 14:05:07 UTC Comment 4

This was fixed for Fedora with the 5.19.6 stable kernel updates.

Note

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