Bug 1928236 (CVE-2021-3411) - CVE-2021-3411 kernel: broken KRETPROBES reports corruption of .text section while running a FTRACE stress tester

Keywords: Security ×

Status: NEW

Alias: CVE-2021-3411

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: 1928462 1928463 1928464 1928465 1928466 1928467

Blocks: 1906597 1928240

TreeView+ depends on / blocked

Reported: 2021-02-12 17:16 UTC by Guilherme de Almeida Suckevicz

Modified: 2022-07-16 03:22 UTC (History)

CC List: 49 users (show)

Fixed In Version: Linux kernel 5.10

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in the Linux kernel. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Clone Of:

Environment:

Last Closed:

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

Guilherme de Almeida Suckevicz 2021-02-12 17:16:15 UTC Description

A violation of memory access flaw was found while detecting a padding of int3 in the linking state in function can_optimize in arch/x86/kernel/kprobes/opt.c. In this problem a local attacker with a special user privilege may cause a threat to a system Integrity and Confidentiality, and may even lead to a denial of service problem.

Here a broken KRETPROBES reports corruption of .text section while running a FTRACE stress tester.

```
[ 5388.259689] Kernel panic - not syncing: [p_lkrg] Kernel Integrity verification failed! Killing the kernel...
[ 5388.269522] CPU: 17 PID: 138522 Comm: kworker/u69:1 Tainted: G        W  OE     5.4.62-std-debug-alt1 #1
[ 5388.278997] Hardware name: Supermicro Super Server/H11DSi, BIOS 1.2 04/15/2019
[ 5388.286243] Workqueue: events_unbound p_check_integrity [p_lkrg]
[ 5388.292255] Call Trace:
[ 5388.294718]  dump_stack+0xac/0xec
[ 5388.298055]  panic+0x119/0x31a
[ 5388.301154]  p_check_integrity.cold+0x1828/0x1e81 [p_lkrg]
[ 5388.306670]  process_one_work+0x2ad/0x5e0
[ 5388.310713]  worker_thread+0x4d/0x3e0
[ 5388.314389]  ? process_one_work+0x5e0/0x5e0
[ 5388.318586]  kthread+0x133/0x150
[ 5388.321832]  ? kthread_mod_delayed_work+0xc0/0xc0
[ 5388.326548]  ret_from_fork+0x27/0x50
[ 5388.330546] Kernel Offset: disabled
[ 5388.339867] ---[ end Kernel panic - not syncing: [p_lkrg] Kernel Integrity verification failed! Killing the kernel... ]---
```

Reference:
http://blog.pi3.com.pl/?p=831

Rohit Keshri 2021-02-14 10:00:23 UTC Comment 5

Mitigation:

Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Rohit Keshri 2021-02-14 10:02:02 UTC Comment 7

External References:

http://blog.pi3.com.pl/?p=831

Note

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