Bug 1888726 (CVE-2020-25656) - CVE-2020-25656 kernel: use-after-free in read in vt_do_kdgkb_ioctl

Keywords: Security ×

Status: CLOSED ERRATA

Alias: CVE-2020-25656

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: 1896773 1896774 1896775 1896776 1896777 ~~1897134~~

Blocks: 1888621

TreeView+ depends on / blocked

Reported: 2020-10-15 15:21 UTC by msiddiqu

Modified: 2021-03-23 19:05 UTC (History)

CC List: 52 users (show)

Fixed In Version: kernel 5.10-rc2

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.

Clone Of:

Environment:

Last Closed: 2021-03-16 19:19:06 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-2021:0856	0	None	None	None	2021-03-16 13:51:07 UTC
Red Hat Product Errata	RHSA-2021:0857	0	None	None	None	2021-03-16 13:52:09 UTC

msiddiqu 2020-10-15 15:21:26 UTC Description

A flaw was found in Linux Kernel, where a race in KDGKBSENT and KDSKBSENT leads to use-after-free read in vt_do_kdgkb_ioctl

References:

https://groups.google.com/g/syzkaller-bugs/c/kZsmxkpq3UI/m/J35PFexWBgAJ?pli=1

msiddiqu 2020-10-19 04:37:37 UTC Comment 1

References:

https://www.openwall.com/lists/oss-security/2020/10/16/1

Alex 2020-11-11 13:30:18 UTC Comment 3

List of patches:

1. Older patches (already applied for 5.9 Kernel):
https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/drivers/tty/vt/keyboard.c?id=6ca03f90527e499dd5e32d6522909e2ad390896b
https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/drivers/tty/vt/keyboard.c?id=82e61c3909db51d91b9d3e2071557b6435018b80

2. Suggested patch for resolving issue:
https://lkml.org/lkml/2020/10/29/528

Alex 2020-11-11 14:13:51 UTC Comment 5

External References:

https://lkml.org/lkml/2020/10/29/528
https://lkml.org/lkml/2020/10/16/84

Petr Matousek 2020-11-12 12:11:09 UTC Comment 7

Created kernel tracking bugs for this issue:

Affects: fedora-all [~~bug 1897134~~]

Fedora Update System 2020-11-16 01:09:02 UTC Comment 8

FEDORA-2020-98ccae320c has been pushed to the Fedora 33 stable repository.
If problem still persists, please make note of it in this bug report.

Fedora Update System 2020-11-16 01:12:45 UTC Comment 9

FEDORA-2020-e211716d08 has been pushed to the Fedora 32 stable repository.
If problem still persists, please make note of it in this bug report.

Alex 2021-02-10 16:42:10 UTC Comment 10

Statement:

This issue is rated as having Moderate impact because of the attack scenario limitation where only local user with access to VT console if at least CAP_SYS_TTY_CONFIG enabled can trigger this issue.

Alex 2021-02-10 16:58:14 UTC Comment 11

For triggering the bug, user needs privileges. At least "CAP_SYS_TTY_CONFIG" needs to be enabled, but this is not the only precondition.
As far as I know, there is no known way today for triggering this until CONFIG_KASAN enabled (that is parameter for runtime memory debugger and usually disabled for production systems).
Means that if parameter CONFIG_KASAN not enabled for the kernel (for rhel* by default disabled), then the bug happens silently (without kernel crash) since read use-after-free usually not easily triggerable.

errata-xmlrpc 2021-03-16 13:51:03 UTC Comment 12

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2021:0856 https://access.redhat.com/errata/RHSA-2021:0856

errata-xmlrpc 2021-03-16 13:52:07 UTC Comment 13

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2021:0857 https://access.redhat.com/errata/RHSA-2021:0857

Product Security DevOps Team 2021-03-16 19:19:06 UTC Comment 14

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-2020-25656