Bug 2069793 (CVE-2022-1158) - CVE-2022-1158 kernel: KVM: cmpxchg_gpte can write to pfns outside the userspace region [NEEDINFO]

Keywords: Security ×

Status: NEW

Alias: CVE-2022-1158

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2122535 2122536 2122537 2122538 2122539 2122541 2122542 2122543 2122544 2122545 2122546 2122547 2122548 2122549 2122550 2122551 ~~2096819~~ 2100245 2100246 2100247 2100248

Blocks: 2069794 2069796

TreeView+ depends on / blocked

Reported: 2022-03-29 17:36 UTC by Marian Rehak

Modified: 2022-09-26 12:29 UTC (History)

CC List: 59 users (show)

Fixed In Version: kernel 5.18

Doc Type: If docs needed, set a value

Doc Text: A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition.

Clone Of:

Environment:

Last Closed:

Flags: mcasquer: needinfo? (pbonzini)

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

Marian Rehak 2022-03-29 17:36:26 UTC Description

Since both vaddr and vm_pgoff are controllable by the user-mode process, writing may exceed the previously mapped guest memory space and trigger exceptions such as UAF.

Marian Rehak 2022-06-14 11:17:06 UTC Comment 2

Created kernel tracking bugs for this issue:

Affects: fedora-all [~~bug 2096819~~]

Justin M. Forbes 2022-06-16 14:15:17 UTC Comment 3

This was fixed for Fedora with the 5.16.19 stable kernel updates.

Mauro Matteo Cascella 2022-06-22 19:44:58 UTC Comment 4

This bug was introduced in kernel upstream version 5.2 with commit [1].
For distros and stable, Paolo Bonzini sent an inline assembly patch that
updates the gPTE using a valid userspace address [2]. With the same method,
Sean Christopherson and Peter Zijlstra introduced macros for CMPXCHG and
replaced cmpxchg_gpte() with __try_cmpxchg_user() [3].

[1] https://github.com/torvalds/linux/commit/bd53cb35a3e9adb73a834a36586e9ad80e877767
[2] https://github.com/torvalds/linux/commit/2a8859f373b0a86f0ece8ec8312607eacf12485d
[3] https://github.com/torvalds/linux/commit/f122dfe4476890d60b8c679128cd2259ec96a24c

Paolo Bonzini 2022-09-22 10:22:26 UTC Comment 14

I suggest using the simpler fix at upstream commit 2a8859f373b0a86f0ece8ec8312607eacf12485d for z-stream.