# Bug 8149 (CVE-2024-24855) - scsi: lpfc的lpfc_unregister_fcf_rescan函数存在竞争条件

| | | | |
|---|---|---|---|
| **Status:** | NEW | **Reported:** | 2024-02-01 17:16 UTC by Shiloong |
| | | **Modified:** | 2024-03-06 09:59 UTC (History) |
| **Alias:** | CVE-2024-24855 | **CC List:** | 2 users (show) |
| **Product:** | ANCK 5.10 Dev | **See Also:** | |
| **Component:** | drivers (show other bugs) drivers | | |
| **Version:** | 5.10.y-16 | | |
| **Hardware:** | All Linux | | |
| **Importance:** | P3-Medium S3-normal | | |
| **Target Milestone:** | --- | | |
| **Assignee:** | GuixinLiu | | |
| **QA Contact:** | shuming | | |
| **URL:** | | | |
| **Whiteboard:** | | | |
| **Keywords:** | | | |
| **Depends on:** | | | |
| **Blocks:** | | | |

| Attachments |
|---|
| Add an attachment (proposed patch, testcase, etc.) |

Note

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

Description

**Shiloong** **2024-02-01 17:16:12 UTC**

上报人信息：
- 白家驹 <baijiaju@buaa.edu.cn>
- 北京航空航天大学网络空间安全学院

成因：
phba->fcf.fcf_flag的写操作需要spinlock phba->hbalock保护，lpfc_unregister_fcf_rescan函数中phba->fcf.fcf_flag = 0语句没有被对应的spinlock保护，可以发生关于phba->fcf.fcf_flag的数据竞争。

危害：
bug触发后，phba->fcf.fcf_flag的置0操作可能被覆盖，phba->fcf.fcf_flag用于记录HBA FCF状态，是lpfc模块的核心变量，决定了驱动函数行为，置0操作被覆盖会导致如lpfc_linkdown、lpfc_work_done等函数发生错误，导致lpfc功能异常，可以用于拒绝服务，甚至触发双重释放等严重的内存问题。

缓解：
- 把lpfc_unregister_fcf_rescan函数中的phba->fcf.fcf_flag |= FCF_INIT_DISC语句两侧添加相应的spin_lock，防止数据竞争。

修复：
补丁已提交给Linux Kernel并被接收，补丁链接：
https://git.kernel.org/pub/scm/linux/kernel/git/next/linux-next.git/commit/?id=0e881c0a4b6146b7e856735226208f48251facd8

Format For Printing - XML - Clone This Bug - Top of page