NVD DB Update

CVE-2024-38605 - Score: 8.8

Components:

linux linux kernel *

Description:

In the Linux kernel, the following vulnerability has been resolved: ALSA: core: Fix NULL module pointer assignment at card init The commit 81033c6b584b ("ALSA: core: Warn on empty module") introduced a WARN_ON() for a NULL module pointer passed at snd_card object creation, and it also wraps the code around it with '#ifdef MODULE'. This works in most cases, but the devils are always in details. "MODULE" is defined when the target code (i.e. the sound core) is built as a module; but this doesn't mean that the caller is also built-in or not. Namely, when only the sound core is built-in (CONFIG_SND=y) while the driver is a module (CONFIG_SND_USB_AUDIO=m), the passed module pointer is ignored even if it's non-NULL, and card->module remains as NULL. This would result in the missing module reference up/down at the device open/close, leading to a race with the code execution after the module removal. For addressing the bug, move the assignment of card->module again out of ifdef. The WARN_ON() is still wrapped with ifdef because the module can be really NULL when all sound drivers are built-in. Note that we keep 'ifdef MODULE' for WARN_ON(), otherwise it would lead to a false-positive NULL module check. Admittedly it won't catch perfectly, i.e. no check is performed when CONFIG_SND=y. But, it's no real problem as it's only for debugging, and the condition is pretty rare.

Main problems:

476 "NULL Pointer Dereference"