

Overall rating: Critical



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware multiple vulnerabilities reported in the Linux Kernel (various versions).

Technical Details

- **Linux Kernel <6.3.2 Remote Use After Free Vulnerability - CVE-2023-35823**
An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.
- **Linux Kernel <6.3.2 Remote Use After Free Vulnerability - CVE-2023-35824**
An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.
- **Linux Kernel <6.3.4 Remote Use After Free Vulnerability - CVE-2023-35825**
An issue was discovered in the Linux kernel before 6.3.4. A use-after-free was found in r592_remove in drivers/memstick/host/r592.c.
- **Linux Kernel <6.3.2 Remote Use After Free Vulnerability - CVE-2023-35826**
An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in cedrus_remove in drivers/staging/media/sunxi/cedrus/cedrus.c.
- **Linux Kernel kernel Remote Use After Free Vulnerability - CVE-2023-35827**
An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.
- **Linux Kernel <6.3.2 Remote Use After Free Vulnerability - CVE-2023-35828**
An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in drivers/usb/gadget/udc/renesas_usb3.c.
- **Linux Kernel <6.3.2 Remote Use After Free Vulnerability - CVE-2023-35829**
An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvddec_remove in drivers/staging/media/rkvddec/rkvddec.c.

These vulnerabilities are rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify [VRM](#) with any questions or concerns you may have.

References

- <https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.2>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=30cf57da176cca80f11df0d9b7f71581fe601389>
- <https://lore.kernel.org/all/49bb0b6a-e669-d4e7-d742-a19d2763e947@xs4all.nl/>
- <https://lore.kernel.org/lkml/20230318085023.832510-1-zyytlz.wz@163.com/t/>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5abda7a16698d4d1f47af1168d8fa2c640116b4a>
- <https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.4>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=63264422785021704c39b38f65a78ab9e4a186d7>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=50d0a7aea4809cef87979d4669911276aa23b71f>
- <https://lore.kernel.org/lkml/cca0b40b-d6f8-54c7-1e46-83cb62d0a2f1@huawei.com/T/>
- <https://www.spinics.net/lists/netdev/msg886947.html>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2b947f8769be8b8181dc795fd292d3e7120f5204>
- <https://lore.kernel.org/all/20230327121700.52d881e0@canb.auug.org.au/>
- <https://lore.kernel.org/lkml/CAJedcCwkuznS1kSTvJXhzPoavcZDWNhNMshi-Ux0spSVRwU=RA@mail.gmail.com/T/>
- <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3228cec23b8b29215e18090c6ba635840190993d>