USN-4749-1: Linux kernel vulnerabilities

Bodong Zhao discovered a use-after-free in the Sun keyboard driver implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2020-25669)

It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service (system crash). (CVE-2020-27815)

Shisong Qin and Bodong Zhao discovered that Speakup screen reader driver in the Linux kernel did not correctly handle setting line discipline in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-27830, CVE-2020-28941)

It was discovered that the memory management subsystem in the Linux kernel did not properly handle copy-on-write operations in some situations. A local attacker could possibly use this to gain unintended write access to read-only memory pages. (CVE-2020-29374)

Michael Kurth and Pawel Wieczorkiewicz discovered that the Xen event processing backend in the Linux kernel did not properly limit the number of events queued. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2020-29568)

Olivier Benjamin and Pawel Wieczorkiewicz discovered a race condition the Xen paravirt block backend in the Linux kernel, leading to a use-after-free vulnerability. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2020-29569)

Jann Horn discovered that the tty subsystem of the Linux kernel did not use consistent locking in some situations, leading to a read-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2020-29660)

Jann Horn discovered a race condition in the tty subsystem of the Linux kernel in the locking for the TIOCSPGRP ioctl(), leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-29661)