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)

USN-4753-1: Linux kernel (OEM) vulnerability

It was discovered that the LIO SCSI target implementation in the Linux
kernel performed insufficient identifier checking in certain XCOPY
requests. An attacker with access to at least one LUN in a multiple
backstore environment could use this to expose sensitive information or
modify data.

USN-4752-1: Linux kernel (OEM) vulnerabilities

Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen discovered
that legacy pairing and secure-connections pairing authentication in the
Bluetooth protocol could allow an unauthenticated user to complete
authentication without pairing credentials via adjacent access. A
physically proximate attacker could use this to impersonate a previously
paired Bluetooth device. (CVE-2020-10135)
Jay Shin discovered that the ext4 file system implementation in the Linux
kernel did not properly handle directory access with broken indexing,
leading to an out-of-bounds read vulnerability. A local attacker could use

this to cause a denial of service (system crash). (CVE-2020-14314)

It was discovered that the block layer implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-15436)

It was discovered that the serial port driver in the Linux kernel did not properly initialize a pointer in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2020-15437)

Andy Nguyen discovered that the Bluetooth HCI event packet parser in the Linux kernel did not properly handle event advertisements of certain sizes, leading to a heap-based buffer overflow. A physically proximate remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-24490)

It was discovered that the NFS client implementation in the Linux kernel did not properly perform bounds checking before copying security labels in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-25212)

It was discovered that the Rados block device (rbd) driver in the Linux kernel did not properly perform privilege checks for access to rbd devices in some situations. A local attacker could use this to map or unmap rbd block devices. (CVE-2020-25284)

It was discovered that the block layer subsystem in the Linux kernel did not properly handle zero-length requests. A local attacker could use this to cause a denial of service. (CVE-2020-25641)

It was discovered that the HDLC PPP implementation in the Linux kernel did not properly validate input in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-25643)

Kiyin (□□) discovered that the perf subsystem in the Linux kernel did not properly deallocate memory in some situations. A privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2020-25704)

It was discovered that the KVM hypervisor in the Linux kernel did not properly handle interrupts in certain situations. A local attacker in a guest VM could possibly use this to cause a denial of service (host system crash). (CVE-2020-27152)

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)

It was discovered that an information leak existed in the syscall implementation in the Linux kernel on 32 bit systems. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-28588)

It was discovered that the framebuffer implementation in the Linux kernel did not properly perform range checks in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-28915)

Jann Horn discovered a race condition in the copy-on-write implementation in the Linux kernel when handling hugepages. A local attacker could use this to gain unintended write access to read-only memory pages. (CVE-2020-29368)

Jann Horn discovered that the mmap implementation in the Linux kernel contained a race condition when handling munmap() operations, 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. (CVE-2020-29369)

Jann Horn discovered that the romfs file system in the Linux kernel did not properly validate file system meta-data, leading to an out-of-bounds read. An attacker could use this to construct a malicious romfs image that, when mounted, exposed sensitive information (kernel memory). (CVE-2020-29371)

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)

It was discovered that a race condition existed that caused the Linux kernel to not properly restrict exit signal delivery. A local attacker could possibly use this to send signals to arbitrary processes. (CVE-2020-35508)

USN-4751-1: Linux kernel vulnerabilities

It was discovered that the console keyboard driver in the Linux kernel contained a race condition. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-25656)
Minh Yuan discovered that the tty driver in the Linux kernel contained race conditions when handling fonts. A local attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2020-25668)

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)

Kiyin (□□) discovered that the perf subsystem in the Linux kernel did not properly deallocate memory in some situations. A privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2020-25704)

Julien Grall discovered that the Xen dom0 event handler 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-2020-27673)

Jinoh Kang discovered that the Xen event channel infrastructure in the Linux kernel contained a race condition. An attacker in guest could possibly use this to cause a denial of service (dom0 crash). (CVE-2020-27675)

Daniel Axtens discovered that PowerPC RTAS implementation in the Linux kernel did not properly restrict memory accesses in some situations. A privileged local attacker could use this to arbitrarily modify kernel memory, potentially bypassing kernel lockdown restrictions. (CVE-2020-27777)

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 a use-after-free vulnerability existed in the infiniband hfi1 device driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2020-27835)

It was discovered that an information leak existed in the syscall implementation in the Linux kernel on 32 bit systems. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-28588)

Minh Yuan discovered that the framebuffer console driver in the Linux kernel did not properly handle fonts in some conditions. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2020-28974)

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)

It was discovered that a race condition existed that caused the Linux kernel to not properly restrict exit signal delivery. A local attacker could possibly use this to send signals to arbitrary processes. (CVE-2020-35508)

USN-4747-2: GNU Screen vulnerability

USN-4747-1 fixed a vulnerability in screen. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

Felix Weinmann discovered that GNU Screen incorrectly handled certain character sequences. A remote attacker could use this issue to cause GNU Screen to crash, resulting in a denial of service, or possibly execute arbitrary code.