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.

USN-4747-1: GNU Screen vulnerability

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.

USN-4746-1: xterm vulnerability

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

USN-4698-2: Dnsmasq regression

USN-4698-1 fixed vulnerabilities in Dnsmasq. The updates introduced
regressions in certain environments related to issues with multiple
queries, and issues with retries. This update fixes the problem.
Original advisory details:

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled
memory when sorting RRsets. A remote attacker could use this issue to cause
Dnsmasq to hang, resulting in a denial of service, or possibly execute
arbitrary code. (CVE-2020-25681, CVE-2020-25687)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled
extracting certain names. A remote attacker could use this issue to cause
Dnsmasq to hang, resulting in a denial of service, or possibly execute
arbitrary code. (CVE-2020-25682, CVE-2020-25683)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly
implemented address/port checks. A remote attacker could use this issue to
perform a cache poisoning attack. (CVE-2020-25684)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly
implemented query resource name checks. A remote attacker could use this

issue to perform a cache poisoning attack. (CVE-2020-25685)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled multiple query requests for the same resource name. A remote attacker could use this issue to perform a cache poisoning attack. (CVE-2020-25686)

It was discovered that Dnsmasq incorrectly handled memory during DHCP response creation. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2019-14834)