

USN-4912-1: Linux kernel (OEM) vulnerabilities

Piotr Krysiuk discovered that the BPF JIT compiler for x86 in the Linux kernel did not properly validate computation of branch displacements in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-29154)

It was discovered that a race condition existed in the binder IPC implementation in the Linux kernel, 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-2020-0423)

It was discovered that the HID multitouch implementation within the Linux kernel did not properly validate input events in some situations. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-0465)

It was discovered that the eventpoll (aka epoll) implementation in the Linux kernel contained a logic error that could lead 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-2020-0466)

It was discovered that a race condition existed in the perf subsystem of the Linux kernel, leading to a use-after-free vulnerability. An attacker with access to the perf subsystem could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-14351)

It was discovered that the frame buffer implementation in the Linux kernel did not properly handle some edge cases in software scrollback. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-14390)

It was discovered that a race condition existed in the hugetlb sysctl implementation in the Linux kernel. A privileged attacker could use this to cause a denial of service (system crash). (CVE-2020-25285)

It was discovered that the GENEVE tunnel implementation in the Linux kernel when combined with IPsec did not properly select IP routes in some situations. An attacker could use this to expose sensitive information (unencrypted network traffic). (CVE-2020-25645)

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)

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)

It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad-hoc SSIDs. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-36158)

Loris Reiff discovered that the BPF implementation in the Linux kernel did not properly validate attributes in the getsockopt BPF hook. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-20194)

Adam Zaborcki discovered that the kprobes subsystem in the Linux kernel did not properly detect linker padding in some situations. A privileged attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2021-3411)

□□ discovered that the NFS implementation in the Linux kernel did not properly prevent access outside of an NFS export that is a subdirectory of a file system. An attacker could possibly use this to bypass NFS access

restrictions. (CVE-2021-3178)