

USN-4884-1: Linux kernel (OEM) vulnerabilities

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)

It was discovered that the priority inheritance futex implementation in the Linux kernel contained a race condition, 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-2021-3347)

It was discovered that the network block device (nbd) driver in the Linux kernel contained a use-after-free vulnerability during device setup. A local attacker with access to the nbd device could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3348)