# USN-4907-1: Linux kernel vulnerabilities

Wen Xu discovered that the xfs file system implementation in the Linux
kernel did not properly validate the number of extents in an inode. An
attacker could use this to construct a malicious xfs image that, when
mounted, could cause a denial of service (system crash).
(CVE-2018-13095)
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)