USN-4910-1: Linux kernel vulnerabilities

Ryota Shiga discovered that the sockopt BPF hooks in the Linux kernel could
allow a user space program to probe for valid kernel addresses. A local
attacker could use this to ease exploitation of another kernel vulnerability. (CVE-2021-20239)
It was discovered that the BPF verifier in the Linux kernel did not
properly handle signed add32 and sub integer overflows. A local attacker
could use this to cause a denial of service (system crash) or possibly
execute arbitrary code. (CVE-2021-20268)

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)

□□ 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)