USN-4909-1: Linux kernel 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)
Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H. Schönherr
discovered that the Xen paravirtualization backend in the Linux kernel did
not properly propagate errors to frontend drivers in some situations. An
attacker in a guest VM could possibly use this to cause a denial of service
(host domain crash). (CVE-2021-26930)

Jan Beulich discovered that multiple Xen backends in the Linux kernel did
not properly handle certain error conditions under paravirtualization. An
attacker in a guest VM could possibly use this to cause a denial of service
(host domain crash). (CVE-2021-26931)

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)