USN-4876-1: Linux kernel vulnerabilities

Olivier Benjamin and Pawel Wieczorkiewicz discovered a race condition the
Xen paravirt block backend in the Linux kernel, leading to a use-after-free
vulnerability. An attacker in a guest VM could use this to cause a denial
of service in the host OS. (CVE-2020-29569)
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)

□□ 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)