

USN-4877-1: Linux kernel vulnerabilities

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)

It was 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)