USN-4887-1: Linux kernel vulnerabilities

De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux
kernel did not properly handle mod32 destination register truncation when
the source register was known to be 0. A local attacker could use this to
expose sensitive information (kernel memory) or possibly execute arbitrary
code. (CVE-2021-3444)
Adam Nichols discovered that heap overflows existed in the iSCSI subsystem
in the Linux kernel. A local attacker could use this to cause a denial of
service (system crash) or possibly execute arbitrary code. (CVE-2021-27365)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not
properly compute a speculative execution limit on pointer arithmetic in
some situations. A local attacker could use this to expose sensitive
information (kernel memory). (CVE-2020-27171)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not
properly apply speculative execution limits on some pointer types. A local
attacker could use this to expose sensitive information (kernel memory).
(CVE-2020-27170)

Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did not properly restrict access to iSCSI transport handles. A local attacker could use this to cause a denial of service or expose sensitive information (kernel pointer addresses). (CVE-2021-27363)

Adam Nichols discovered that an out-of-bounds read existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2021-27364)