USN-4891-1: OpenSSL vulnerability

It was discovered that OpenSSL incorrectly handled certain renegotiation
ClientHello messages. A remote attacker could use this issue to cause
OpenSSL to crash, resulting in a denial of service, or possibly execute
arbitrary code.

USN-4889-1: Linux kernel vulnerabilities

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)
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)

USN-4890-1: Linux kernel vulnerabilities

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)

USN-4888-1: ldb vulnerabilities

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain LDAP attributes. A remote attacker could possibly use this

issue to cause the LDAP server to crash, resulting in a denial of service.
(CVE-2021-20277)
Douglas Bagnall discovered that ldb, when used with Samba, incorrectly
handled certain DN strings. A remote attacker could use this issue to
cause the LDAP server to crash, resulting in a denial of service, or
possibly execute arbitrary code. (CVE-2020-27840)

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)