USN-4738-1: OpenSSL vulnerabilities

Paul Kehrer discovered that OpenSSL incorrectly handled certain input
lengths in EVP functions. A remote attacker could possibly use this issue
to cause OpenSSL to crash, resulting in a denial of service. (CVE-2021-23840)
Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer
fields. A remote attacker could possibly use this issue to cause OpenSSL to
crash, resulting in a denial of service. (CVE-2021-23841)