USN-4745-1: OpenSSL vulnerabilities

David Benjamin discovered that OpenSSL incorrectly handled comparing
certificates containing a EDIPartyName name type. A remote attacker could
possibly use this issue to cause OpenSSL to crash, resulting in a denial of
service. (CVE-2020-1971)
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)