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)

USN-4467-3: QEMU regression

USN-4467-1 fixed vulnerabilities in QEMU. The fix for CVE-2020-13754
introduced a regression in certain environments. This update fixes the
problem.
We apologize for the inconvenience.

Original advisory details:

Ren Ding, Hanqing Zhao, Alexander Bulekov, and Anatoly Trosinenko
discovered that the QEMU incorrectly handled certain msi-x mmio operations.
An attacker inside a guest could possibly use this issue to cause QEMU to

crash, resulting in a denial of service. (CVE-2020-13754)

USN-4744-1: OpenLDAP vulnerability

Pasi Saarinen discovered that OpenLDAP incorrectly handled certain short
timestamps. A remote attacker could possibly use this issue to cause
OpenLDAP to crash, resulting in a denial of service.

USN-4743-1: GDK-PixBuf vulnerability

It was discovered that the GDK-PixBuf library did not properly handle
certain GIF images. If an user or automated system were tricked into
opening a specially crafted GIF file, a remote attacker could use this flaw
to cause GDK-PixBuf to crash, resulting in a denial of service.

USN-4742-1: Django vulnerability

It was discovered that Django incorrectly accepted semicolons as query
parameters. A remote attacker could possibly use this issue to perform a
Web Cache Poisoning attack.