USN-4903-1: curl vulnerability

Viktor Szakats discovered that curl did not strip off user credentials
from referrer header fields. A remote attacker could possibly use this
issue to obtain sensitive information.

USN-4561-2: Rack vulnerabilities

USN-4561-1 fixed vulnerabilities in Rack. This update provides the
corresponding update for Ubuntu 16.04 LTS, Ubuntu 20.04 LTS and Ubuntu 20.10.
Original advisory details:

It was discovered that Rack incorrectly handled certain paths. An attacker
could possibly use this issue to obtain sensitive information. This issue
only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.
(CVE-2020-8161)

It was discovered that Rack incorrectly validated cookies. An attacker
could possibly use this issue to forge a secure cookie. (CVE-2020-8184)

USN-4902-1: Django vulnerability

Dennis Brinkrolf discovered that Django incorrectly handled certain
filenames. A remote attacker could possibly use this issue to create or
overwrite files in unexpected directories.

USN-4901-1: Linux kernel (Trusty HWE) 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)
It was discovered that the LIO SCSI target implementation in the Linux
kernel performed insufficient identifier checking in certain XCOPY
requests. An attacker with access to at least one LUN in a multiple
backstore environment could use this to expose sensitive information or
modify data. (CVE-2020-28374)

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-4899-1: SpamAssassin vulnerability

Damian Lukowski discovered that SpamAssassin incorrectly handled certain CF
files. If a user or automated system were tricked into using a specially-
crafted CF file, a remote attacker could possibly run arbitrary code.