USN-4876-1: Linux kernel vulnerabilities

Olivier Benjamin and Pawel Wieczorkiewicz discovered a race condition the
Xen paravirt block backend in the Linux kernel, leading to a use-after-free
vulnerability. An attacker in a guest VM could use this to cause a denial
of service in the host OS. (CVE-2020-29569)
It was discovered that the Marvell WiFi-Ex device driver in the Linux
kernel did not properly validate ad-hoc SSIDs. A local attacker could use
this to cause a denial of service (system crash) or possibly execute
arbitrary code. (CVE-2020-36158)

□□ discovered that the NFS implementation in the Linux kernel did not
properly prevent access outside of an NFS export that is a subdirectory of
a file system. An attacker could possibly use this to bypass NFS access
restrictions. (CVE-2021-3178)

USN-4764-1: GLib vulnerability

It was discovered that GLib incorrectly handled certain symlinks when
replacing files. If a user or automated system were tricked

into extracting
a specially crafted file with File Roller, a remote attacker could possibly
create files outside of the intended directory.

USN-4754-3: Python vulnerabilities

USN-4754-1 fixed vulnerabilities in Python. This update provides
the corresponding updates for Ubuntu 18.04 ESM and Ubuntu 20.04 ESM.
In the case of Python 2.7 for 20.04 ESM, these additional fixes are included:

It was dicovered that Python allowed remote attackers to cause a denial of
service (resource consumption) via a ZIP bomb. (CVE-2019-9674)

It was discovered that Python had potentially misleading information about
whether sorting occurs. This fix updates the documentation about it.
(CVE-2019-17514)

It was discovered that Python incorrectly handled certain TAR archives.
An attacker could possibly use this issue to cause a denial of service.
(CVE-2019-20907)

It was discovered that Python allowed an HTTP server to conduct Regular
Expression Denial of Service (ReDoS) attacks against a client because of

urllib.request.AbstractBasicAuthHandler catastrophic backtracking.
(CVE-2020-8492)

It was discovered that Python allowed CRLF injection if the attacker controls
the HTTP request method, as demonstrated by inserting CR and LF control
characters in the first argument of HTTPConnection.request.
(CVE-2020-26116)

Original advisory details:

It was discovered that Python incorrectly handled certain inputs.
An attacker could possibly use this issue to execute arbitrary code
or cause a denial of service. (CVE-2020-27619, CVE-2021-3177)

USN-4763-1: Pillow vulnerabilities

It was discovered that Pillow incorrectly handled certain Tiff image files.
If a user or automated system were tricked into opening a specially-crafted
Tiff file, a remote attacker could cause Pillow to crash, resulting in a
denial of service, or possibly execute arbitrary code. This issue only
affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2021-25289, CVE-2021-25291)
It was discovered that Pillow incorrectly handled certain Tiff image files.

If a user or automated system were tricked into opening a specially-crafted
Tiff file, a remote attacker could cause Pillow to crash, resulting in a
denial of service, or possibly execute arbitrary code. (CVE-2021-25290)

It was discovered that Pillow incorrectly handled certain PDF files. If a
user or automated system were tricked into opening a specially-crafted
PDF file, a remote attacker could cause Pillow to hang, resulting in a
denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04
LTS, and Ubuntu 20.10. (CVE-2021-25292)

It was discovered that Pillow incorrectly handled certain SGI image files.
If a user or automated system were tricked into opening a specially-crafted
SGI file, a remote attacker could possibly cause Pillow to crash,
resulting in a denial of service. This issue only affected Ubuntu 18.04
LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-25293)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that
Pillow incorrectly handled certain BLP files. If a user or automated system
were tricked into opening a specially-crafted BLP file, a remote attacker
could possibly cause Pillow to consume resources, resulting in a denial of
service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and
Ubuntu 20.10. (CVE-2021-27921)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that
Pillow incorrectly handled certain ICNS files. If a user or automated
system were tricked into opening a specially-crafted ICNS file, a remote
attacker could possibly cause Pillow to consume resources, resulting in a
denial of service. (CVE-2021-27922)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that
Pillow incorrectly handled certain ICO files. If a user or automated
system were tricked into opening a specially-crafted ICO file, a remote
attacker could possibly cause Pillow to consume resources, resulting in a
denial of service. (CVE-2021-27922)

USN-4762-1: OpenSSH vulnerability

It was discovered that the OpenSSH ssh-agent incorrectly handled memory. A
remote attacker able to connect to the agent could use this issue to cause
it to crash, resulting in a denial of service, or possibly execute
arbitrary code.