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)