USN-4898-1: curl vulnerabilities

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. (CVE-2021-22876)
Mingtao Yang discovered that curl incorrectly handled session tickets when
using an HTTPS proxy. A remote attacker in control of an HTTPS proxy could
use this issue to bypass certificate checks and intercept communications.
This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10.
(CVE-2021-22890)

USN-4897-1: Pygments vulnerability

Ben Caller discovered that Pygments incorrectly handled parsing certain
files. If a user or automated system were tricked into parsing a specially
crafted file, a remote attacker could cause Pygments to hang or consume
resources, resulting in a denial of service.

USN-4896-1: lxml vulnerability

It was discovered that lxml incorrectly handled certain HTML attributes. A
remote attacker could possibly use this issue to perform cross-site
scripting (XSS) attacks.

USN-4895-1: Squid vulnerabilities

Alex Rousskov and Amit Klein discovered that Squid incorrectly handled
certain Content-Length headers. A remote attacker could possibly use this
issue to perform an HTTP request smuggling attack, resulting in cache
poisoning. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-15049)
Jianjun Chen discovered that Squid incorrectly validated certain input. A
remote attacker could use this issue to perform HTTP Request Smuggling and
possibly access services forbidden by the security controls.
(CVE-2020-25097)

USN-4894-1: WebKitGTK vulnerabilities

A large number of security issues were discovered in the WebKitGTK Web and
JavaScript engines. If a user were tricked into viewing a malicious
website, a remote attacker could exploit a variety of issues related to web
browser security, including cross-site scripting attacks, denial of service
attacks, and arbitrary code execution.