USN-4734-1: wpa_supplicant and hostapd vulnerabilities

It was discovered that wpa_supplicant did not properly handle P2P
(Wi-Fi Direct) group information in some situations, leading to a
heap overflow. A physically proximate attacker could use this to cause a
denial of service or possibly execute arbitrary code. (CVE-2021-0326)
It was discovered that hostapd did not properly handle UPnP subscribe
messages in some circumstances. An attacker could use this to cause a
denial of service. (CVE-2020-12695)

USN-4733-1: GNOME Autoar vulnerability

Yiğit Can Yılmaz discovered that GNOME Autoar could extract files outside
of the intended directory. If a user were tricked into extracting a
specially crafted archive, a remote attacker could create files in
arbitrary locations, possibly leading to code execution.

USN-4732-1: SQLite vulnerability

It was discovered that SQLite incorrectly handled certain sub-queries. An
attacker could use this issue to cause SQLite to crash, resulting in a
denial of service, or possibly execute arbitrary code.

USN-4730-1: PostSRSd vulnerability

It was discovered that PostSRSd mishandled certain input. A remote attacker
could use this vulnerability to cause a denial of service via a long timestamp
tag in an SRS address.

USN-4731-1: JUnit 4 vulnerability

It was discovered that JUnit 4 contains a local information disclosure
vulnerability. An attacker could possibly use this issue to obtain sensitive
information.