

# 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)