USN-4698-2: Dnsmasq regression

USN-4698-1 fixed vulnerabilities in Dnsmasq. The updates introduced
regressions in certain environments related to issues with multiple
queries, and issues with retries. This update fixes the problem.
Original advisory details:

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled
memory when sorting RRsets. A remote attacker could use this issue to cause
Dnsmasq to hang, resulting in a denial of service, or possibly execute
arbitrary code. (CVE-2020-25681, CVE-2020-25687)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled
extracting certain names. A remote attacker could use this issue to cause
Dnsmasq to hang, resulting in a denial of service, or possibly execute
arbitrary code. (CVE-2020-25682, CVE-2020-25683)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly
implemented address/port checks. A remote attacker could use this issue to
perform a cache poisoning attack. (CVE-2020-25684)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly
implemented query resource name checks. A remote attacker could use this

issue to perform a cache poisoning attack. (CVE-2020-25685)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled multiple query requests for the same resource name. A remote attacker could use this issue to perform a cache poisoning attack. (CVE-2020-25686)

It was discovered that Dnsmasq incorrectly handled memory during DHCP response creation. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2019-14834)