Google found 7 security bugs on the famous network software Dnsmasq

Security researchers have found seven security holes on the Dnsmasq network service software, three of which allow remote code execution and hijack computers.

Security researchers have found seven security holes on the Dnsmasq network service software, three of which allow remote code execution and hijack computers.

Dnsmasq is a small network tool used by many users, providing a DNS Forwarder, DHCP server (Dynamic Host Configuration Protocol), Route Ads and a network restart service for Small network.

Dnsmasq is preinstalled on many devices and OS, including Linux kernels like Ubuntu and Debian, routers, mobile phones, and IoT devices. Shodan testing with Dnsmasq shows that about 1.1 million devices in the world are installing Dnsmasq.

Currently, Google's research team has discovered seven security flaws, including DNS-related errors for remote code execution, information leakage and service rejection errors via DNS or DHCP.

Security vulnerability on Dnsmasq network service software

In 7 errors, 3 errors can execute remote code, 3 errors to deny service and 1 error can steal information.

All errors have been patched in Dnsmasq 2.78, users should update as quickly as possible. Because the vulnerability has been fixed, Google researchers detailed the PoC code for each vulnerability.

Google has updated the affected services and released security updates for Android partners during the October security update. Other affected Google services have also been updated.