Critical DNS leakage vulnerability in Strongswan mobile VPN client

(CVE-2023-##)

by Robert Hörr (e-mail: robert.hoerr@telekom.de)
(Security Evaluators of the Telekom Security Evaluation Facility)

A new critical leakage vulnerability (CVE-2023-##) was discovered in the Strongswan mobile VPN client (versions 2.4.2 – 2.3.3, https://docs.strongswan.org/docs/5.9/os/androidVpnClient.html) by Security Evaluators of Telekom Security with modern fuzzing methods. The vulnerability leaks some DNS data of the internal network, which is secured by the VPN, even Strongswan is configured with an internal DNS server. An attacker can occupy the Wifi-Router and reads this data. In worst-case, the attacker can inject crafted data into the mobile device.

What is Strongswan?

Strongswan is a complex client- and server VPN implementation in C. A VPN secures the network data traffic between two endpoints. No other third person could read or change the secured traffic. But it is known that Strongswan leaks in some cases. For example, the "Tunnel Shunting" problem shows this (https://docs.strongswan.org/docs/5.9/howtos/securityRecommendations.html#_tunnel_shunting). This report describes another leakage.

How was the vulnerability discovered?

Computer software is becoming more complex. So, it is almost impossible to perform a complete source code review with reasonable coverage. For this reason, modern fuzzing methods are used to discover vulnerabilities. The fuzzing methods include, among other things, AFL, libFuzzer, Jazzer and AdressSanitizer. The tools AFL, Jazzer and libFuzzer are code coverage based fuzzer which are the next generation of fuzzing tools. Strongswan was fuzzed using these fuzzing methods. Some tests found the reported leakage in this report.

What kind of leakage is that?

The Strongswan mobile client leaks the internal DNS traffic which must be secured. The device sends the DNS requests into the local network and not into the VPN. In this case, the DNS traffic is not secure and other third parties can read it. For example, the internal DNS host names of the DNS requests are leaked.

The reason for this leakage could be the following modification from the changelog:

"DNS servers are now explicitly applied whenever a TUN device is created (instead of only when the IKE_SA is established), this ensures that the correct DNS servers are used if the CHILD_SA gets explicitly deleted by the server and recreated by the client."

How is the test setup and process?

The test device is a Samsung S22 which is connected to the Mikrotik Wifi-Router "hAP lite TC". This device is configured in the following way:

- Strongswan version 2.4.2
- "Block connections without VPN" is enabled (Android setting)
- VPN-Type: IKEv2 EAP-TLS (Certificate) (Strongswan setting)
- DNS-Servers: 8.8.4.4 or 192.168.3.5 (Strongswan setting)
- "All applications use the VPN" is enabled (Strongswan setting)

The device starts and establishes the VPN. During this process, the device sends DNS requests out of the VPN.

How is the vulnerability exploitable by an attacker?
An attack can occupy the local Wifi-Router and reads the received DNS requests. So, the hacker gets the internal network host names. These names contain usually the server names, for example exchange. The attacker learns the used severs of the internal network. The hacker could build up the same servers in the local network environment and adds the learned DNS server names to the DNS server of the local Wifi-Router. The device could connect to these local servers if there are other leakages like “Tunnel Shunting”. In worst-case, the device sends sensitive information to these fake servers.