Advisory on the TunnelCrack vulnerabilities (VU#563667)

The Website tunnelcrack.mathyvanhoef.com describes two general classes of attacks against VPN clients, by which an attacker can achieve that network traffic from the user's computer (PC, notebook, smartphone), which is actually intended for the VPN tunnel, leaks outside the VPN tunnel and is sent unencrypted to the local, respectively public network.

Those attacks utilize the common practice of VPN clients to use so-called routing tables of the operating system to determine which network traffic is to be sent through the tunnel and which not. Even without split-tunnelling configuration, there are typically two exceptions for specific types of network traffic, which are not routed through the tunnel:

- network traffic sent to and from the local network (LocalNet exception)
- network traffic sent to and from the VPN server (ServerIP exception)

The LocalNet exception is a convenience feature which ensures for example that the user working from home can still connect to the local network printer even if the VPN tunnel is established.
The ServerIP exception is necessary to ensure that already encrypted VPN network traffic is sent directly to the VPN server and not reencrypted, which would create an endless loop.
Corresponding to the two exception types they present LocalNet and ServerIP attacks.

LocalNet attacks

To perform a LocalNet attack, the attacker needs to control the local network. Typically, this can happen if the user connects to an untrusted wireless network which is controlled by the attacker.

The objective of the attack is to leak the network traffic from the client to a specific targeted server so that the connection does not go through the VPN tunnel but bypasses the tunnel unencrypted. When the client computer connects to the wireless network, it receives an IP address and netmask for the local subnet.

The attacker chooses the address range such that client and server computer belong to the same subnet, whence the LocalNet exception applies.

Depending on the outcome of the attack, two cases can be distinguished.

LocalNet attack resulting in traffic leak (CVE-2023-36672)

This is the main variant in which the attacker fully achieves his goal: the LocalNet exception applies and all network traffic from the user's computer to the targeted server is sent unprotected to the access point, bypassing the VPN tunnel.

Note: *As long as the communication with the server takes place using a protected protocol (e.g., TLS or SSH), the attacker does not get to see the unencrypted data. However, he still obtains valuable meta information like the IP addresses of the participating peers or which communication protocols are used.*

LocalNet-attack resultin in traffic blocking (CVE-2023-35838)

In this subvariant the network traffic does not leak, but instead it is blocked by the VPN client or some firewall.

The attacker is not able to eavesdrop on the traffic however, he still can selectively block traffic to specific servers without being noticed. Therefore, this variant is also considered a (low level) security risk by the researchers. As an example, they mention the case of a security camera, which is not able to connect to its server. (A similar use-case would be to prevent security updates or updates of virus signatures by blocking the update server.)

Note: *For some VPN clients, the blocking occurs because they apply he LocalNet exception only if the local network is assigned a private IP address range according to RFC 1918. This countermeasure however provides only limited protection against leaks and is only effective if the target computer has a public IP address, not a private IP address from the company's intranet.*

Countermeasures against LocalNet attacks

LANCOM Systems suggests the following countermeasures for the Advanced VPN Clients:

LANCOM Advanced VPN Client for Windows

For the LANCOM Advanced VPN Client for Windows, the LocalNet attack can be prevented by enabling the “Full Local Network Enclosure Mode” option. As a result, all network traffic will be sent through the tunnel.

Alternatively, the integrated Advanced VPN Client Firewall can be configured such that only VPN traffic is allowed outside the tunnel (using the “Permit IPsec protocol” firewall option), with dedicated exceptions for, e.g., the local network printer. Please be aware that those rules could lead to undetected blocking of important network traffic (CVE-2023-35838). Against this problem, you need to take separate countermeasures.

LANCOM Advanced VPN Client for macOS

For the LANCOM Advanced VPN Client for macOS, the LocalNet attack can be prevented only partially by enabling the “Full Local Network Enclosure Mode” option. Network traffic to and from the standard gateway will not be routed into the VPN tunnel.

Alternatively, a third-party firewall can be configured such that only VPN traffic is allowed outside the tunnel, with dedicated exceptions for, e.g., the local network printer. Please be aware that those rules could lead to undetected blocking of important network traffic (CVE-2023-35838). Against this problem, you need to take separate countermeasures.

ServerIP attacks

The objective of the attack is to leak the network traffic from the client to a specific targeted server so that the connection does not go through the VPN tunnel but bypasses the tunnel unencrypted by utilizing the ServerIP exception. Essentially, there are two variants of the attack, with different impact.

Note: *For simplicity, we assume in the following that the attacker controls the access point. However, the requirements for the ServerIP attack can be weakened, see section 3: Threat Model of the original publication.*

ServerIP attack resulting in traffic leak to arbitrary IP addresses (CVE-2023-36673)

The main variant requires that the attacker is able to manipulate the IP address under which the client uses to connect to the VPN server. This is the case for example if the VPN client uses a plaintext DNS request to obtain the IP address of the VPN server. In this case the attacker can spoof the IP address of the VPN server to make it equal to the IP address of the targeted server.

To enable the user to successfully establish a VPN connection in spite of the DNS spoofing, the attacker redirects all VPN traffic to and from the original VPN server. As soon as the tunnel is established, the ServerIP exception applies and the entire traffic to and from the targeted server leaks outside the tunnel. The user won't be able to tell the difference, because the VPN tunnel is established and all network traffic, except for the targeted server, are routed as usual.

ServerIP attack resulting in traffic leak to IP address of VPN server (CVE-2023-36671)

If the attacker is not able to manipulate the IP address of the VPN server, for example because it is configured explicitly in the VPN configuration, he does not have many options to exploit the ServerIP exception, because except for VPN traffic there is normally no direct communication between client and VPN server.

The attacker however still has the possibility to learn the public IP address of a user who visits a targeted site via VPN. This so-called deanonymization attack poses a security risk mainly for users which use VPN services to protect their anonymity and for censorship circumvention, and is therefore of little relevance for the typical use-case of LANCOM VPN products, where the VPN connection is primarily used for secure access to company resources. The details of this attack can be found in Section 4.2.1 of the original publication.

ServerIP attack resulting in traffic blocking

This case is analogue to CVE-2023-35838, with even less options for the attacker to exploit it usefully. Therefore, no separate CVE number has been assigned to it by the authors.

Countermeasures against ServerIP attacks

LANCOM Systems suggests the following countermeasures for the Advanced VPN Clients:

LANCOM Advanced VPN Client for Windows

The traffic leak to arbitrary IP addresses (CVE-2023-36673) can be prevented by configuring an IP address instead of a domain name in the VPN configuration. Authenticated DNS variants (DNSSEC) are not supported yet.

Additionally, the integrated Advanced VPN Client Firewall can be configured such that only VPN traffic is allowed outside the VPN tunnel. This can be achieved by setting the “Permit IPsec protocol” firewall option and removing all other firewall rules.

LANCOM Advanced VPN Client for macOS

The traffic leak to arbitrary IP addresses (CVE-2023-36673) can be prevented by configuring an IP address instead of a domain name in the VPN configuration. Authenticated DNS variants (DNSSEC) are not supported yet.

Additionally, a third-party firewall can be configured such that only the VPN protocols are allowed outside the VPN tunnel, which are ISAKMP (UDP port 500) and IPsec NAT-T (UDP port 4500).

Source:

NCP engineering GmbH

Dombühler Str. 2

90449 Nürnberg

Germany

https://www.ncp-e.com/