Advisory

TunnelCrack Vulnerabilities (VU#563667)

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 access network traffic from the user's computer (PC, notebook, smartphone), which is intended for the VPN tunnel. These attacks can cause the traffic to inadmissibly bypassthe VPN tunnel and be transmitted unencrypted over the local or public network.

These attacks make use of the common practice among VPN clients, where the routing tables of the operating system are used to decide which network traffic should be sent through the tunnel and which should not. Even if a split-tunnelling configuration is not enabled, there are usually two exceptions for certain types of network traffic that 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 that ensures, for example, users working from home to continue to connect to the local network printer even if the VPN tunnel is active.

The ServerIP exception is required to ensure that already encrypted VPN network traffic is sent directly to the VPN server, and not re-encrypted, as this would result in an endless loop.

A differentiation is made between LocalNet and ServerIP attacks according to these two exception types.

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 controlled by the attacker.

The objective of the attack is to redirect the network traffic from the client to a specific targeted server so that the connection does not go through the VPN tunnel, but instead bypasses the tunnel unencrypted. When the client computer connects to the wireless network, it receives an IP address and netmask for the local subnet via DHCP. The attacker chooses the address range such that client and target server computer are in the same subnet, from where 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 primary variant in which an attacker successfully achieves their goal by taking advantage of the LocalNet exception. This results in all network traffic between the user's computer and the targeted server being sent without protection to the access point, effectively 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. Nevertheless, they still gain access to valuable meta information such as the IP addresses of the participating peers or which communication protocols are used.*

LocalNet Attack Resulting in Traffic Blocking (CVE-2023-35838)

In this secondary variant, the network traffic is not diverted, but blocked by the VPN client or a firewall.

This means that the attacker cannot eavesdrop on the data traffic to the target computer, but they still have the option of blocking the data traffic to this target computer without being noticed. Therefore, researchers have identified this variant as a low-level security threat. An example that was given was a security camera that cannot link up with its server. (Another comparable scenario is hindering security or virus signature file updates by blocking the update server.)

Note: Some VPN clients may experience blocking because they only apply the LocalNet exception when the local network is assigned a private IP address range as specified by RFC 1918. However, this countermeasure offers only limited protection against data leakage and is effective only if the target computer is a server with a public IP address and not a server with a private IP address from the company's intranet.

Countermeasures Against LocalNet Attacks

NCP suggests the following countermeasures for the NCP Secure Clients:

NCP Secure Client for Windows

For the NCP Windows Client, 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 NCP Secure Windows Client Firewall can be configured in such a way that only VPN traffic is allowed outside the tunnel (using the “Permit IPsec protocol” firewall option), with dedicated exceptions for example, the local network printer. Please be aware that those rules could lead to undetected blocking of important network traffic (CVE-2023-35838) which will require to other Countermeasures to be taken. .

NCP Secure Client for macOS

For the NCP macOS Client, the LocalNet attack can only partially be prevented 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 so that only VPN traffic is allowed outside the tunnel, with dedicated exceptions for example, the local network printer. Please be aware that those rules could lead to undetected blocking of important network traffic (CVE-2023-35838) a situation which may require to be addressed separately.

NCP Secure Client for Android

The NCP Android Client generally does not route any network traffic into the local subnet, it is not vulnerable to the LocalNet attack.

NCP Secure Client for iOS

For the NCP iOS Client, the “Full Local Network Enclosure Mode” has no function, for traffic is always routed past the VPN tunnel. To ensure safety and security, if users are not using an installable third-party firewall, they should only connect to trusted wireless networks or use mobile networks if they are not using a third-party firewall.

To meet the different requirements for working in trusted and untrusted environments, NCP advises to use different VPN link profiles, for example. one with and one without the “Full Local Network Enclosure Mode” option set. Additionally, the NCP firewall supports the “Home Zone” feature to differentiate between your home network and public networks.

ServerIP Attacks

Here, too, the objective of the attack is to redirect the network traffic from the client to a specific target server so that the connection does not go through the VPN tunnel, but instead bypasses the tunnel unencrypted by utilizing the ServerIP exception.

Essentially, there are two variants of the attack, that impact differently,

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

ServerIP Attack Resulting in Traffic Leak to Arbitrary IP Adresses (CVE-2023-36673)

The primary variant requires that the attacker can manipulate the IP address with which the client uses to connect to the VPN server. This is the case, for example, if the VPN client uses an insecure 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 the IP address of their target server.

To enable the user to successfully establish a VPN connection despite 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 causes all traffic to and from the destination machine to be sent past the tunnel. The user usually does not notice this, because the VPN tunnel is up and all network connections except for the target computer server are routed through the tunnel normally.

ServerIP Attack Resulting in Traffic Leak to the IP Address of the VPN-Server (CVE-2023-36671)

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

The attacker however still has the possibility to learn the public IP address of a user who visits certain websites. This so-called deanonymization attack poses a security risk mainly for users who use VPN services to protect their anonymity and for censorship circumvention and is of little relevance for the typical use-case of NCP 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 analogous to CVE-2023-35838 but provides fewer opportunities for the attacker to exploit it usefully. Therefore, no separate CVE number has been assigned to it by the authors.

Countermeasures against ServerIP Attacks

NCP suggests the following countermeasures for the NCP Secure Clients:

NCP Secure 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 NCP Secure 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 from the NCP specific client firewall.

NCP Secure 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.

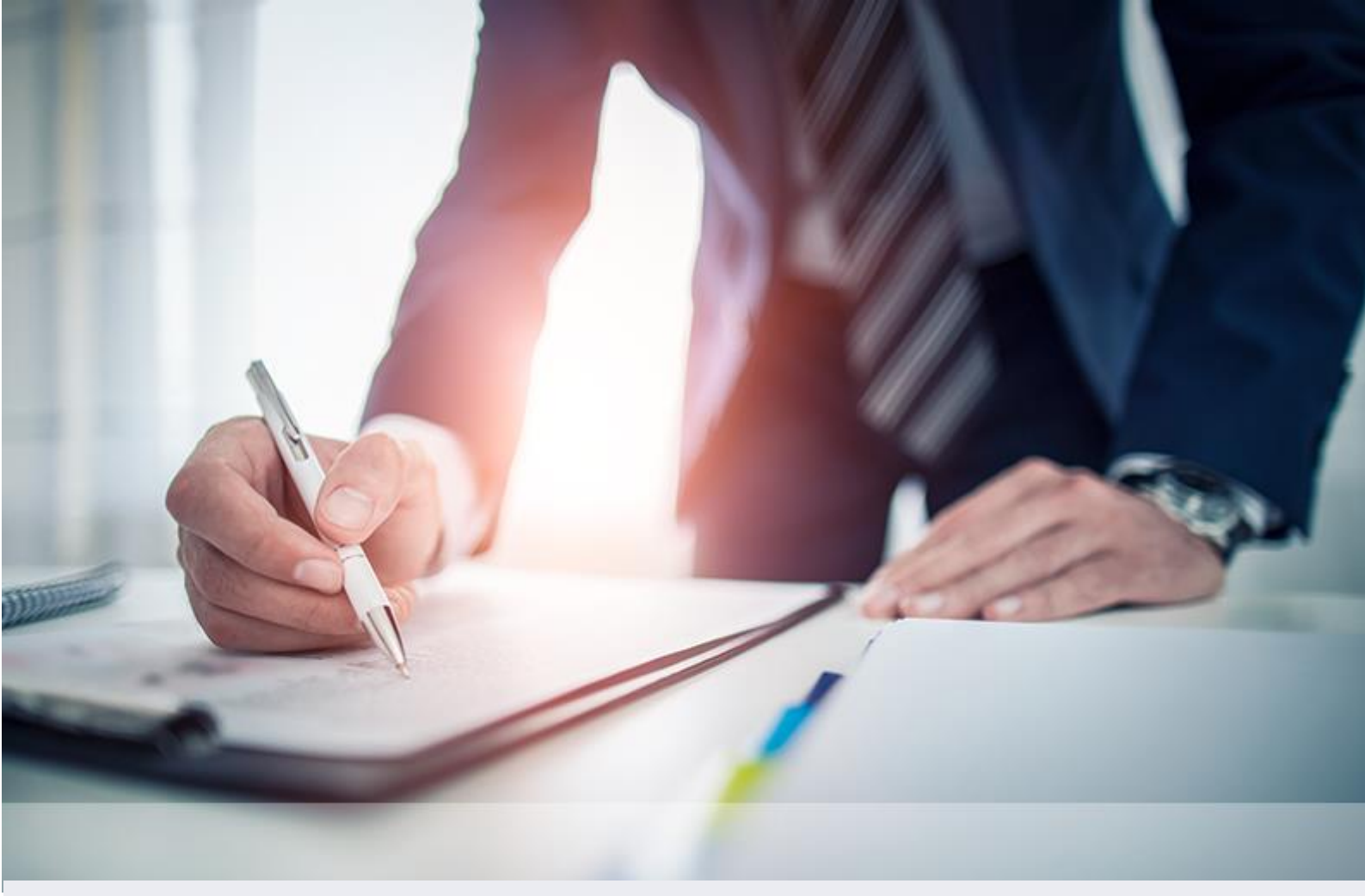
Additionally, a third-party firewall can be configured such that only the VPN protocols are allowed outside the VPN tunnel. These protoccols are ISAKMP (UDP port 500) and IPsec NAT-T (UDP port 4500).

NCP Secure Client for Android

With the NCP Android client, the configured destination address of the VPN server can only be reachable through the VPN tunnel. It is thus not vulnerable to the serverIP attacks.

NCP Secure Client for iOS

With the NCP iOS client, the configured destination address of the VPN server can only be reached through the VPN tunnel. It is thus not vulnerable to the ServerIP attacks.



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968 0
support@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
helpdesk@ncp-e.com
www.ncp-e.com