Advisory

Tunnelvision Vulnerability (CVE-2024-3661)

Advisory on the Tunnelvision Vulnerability (CVE-2024-3661)

The vulnerability discovered by the "Leviathan Security Group" called "Tunnelvision" (CVE-2024-3661) targets remote workstations or networks connected via VPN. The attack is not carried out directly on an existing VPN client, but on the routing in the respective operating system.

Due to the implementation- and vendor-independent nature of the attack, all remote workstations with NCP VPN clients are also affected, except on the Android platform.

Attack method

The attacker imitates a DHCP server in the remote user's network, which manipulates the routing table on the user computer using DHCP option 121. The aim of this manipulation is to ensure that data is not sent via the standard route through the VPN tunnel, but is instead routed past the VPN tunnel.

Connections that are end-to-end encrypted within the VPN tunnel, such as normal website calls via HTTPS or TLS, can still not be decrypted. Communication that is sent unencrypted through the VPN tunnel could be intercepted by the attack. In addition, metadata and information can be leaked via the internal VPN network, such as IP addresses.

Obfuscating or anonymizing VPNs, which are offered commercially in large numbers, are disabled by the attack; communication then no longer takes place through the VPN tunnel.

VPNs that are used in enterprise environments to access private computer networks, as is often the case with NCP customers, are less affected by the attack, as the connection targets are not accessible via the Internet (outside the VPN tunnel); in this case, the attackers could only access the initial message for establishing the connection, further communication with the private computer network would not take place.

Mitigations

Measures to ward off or prevent the attack:

- Deactivation of DHCP and use of permanently assigned IP addresses
- Do not use "split tunneling", if available "forward local networks in the tunnel", and use a firewall to allow only VPN traffic (please refer to the notes "Problems with Firewall Rule Mitigations" in 1)).

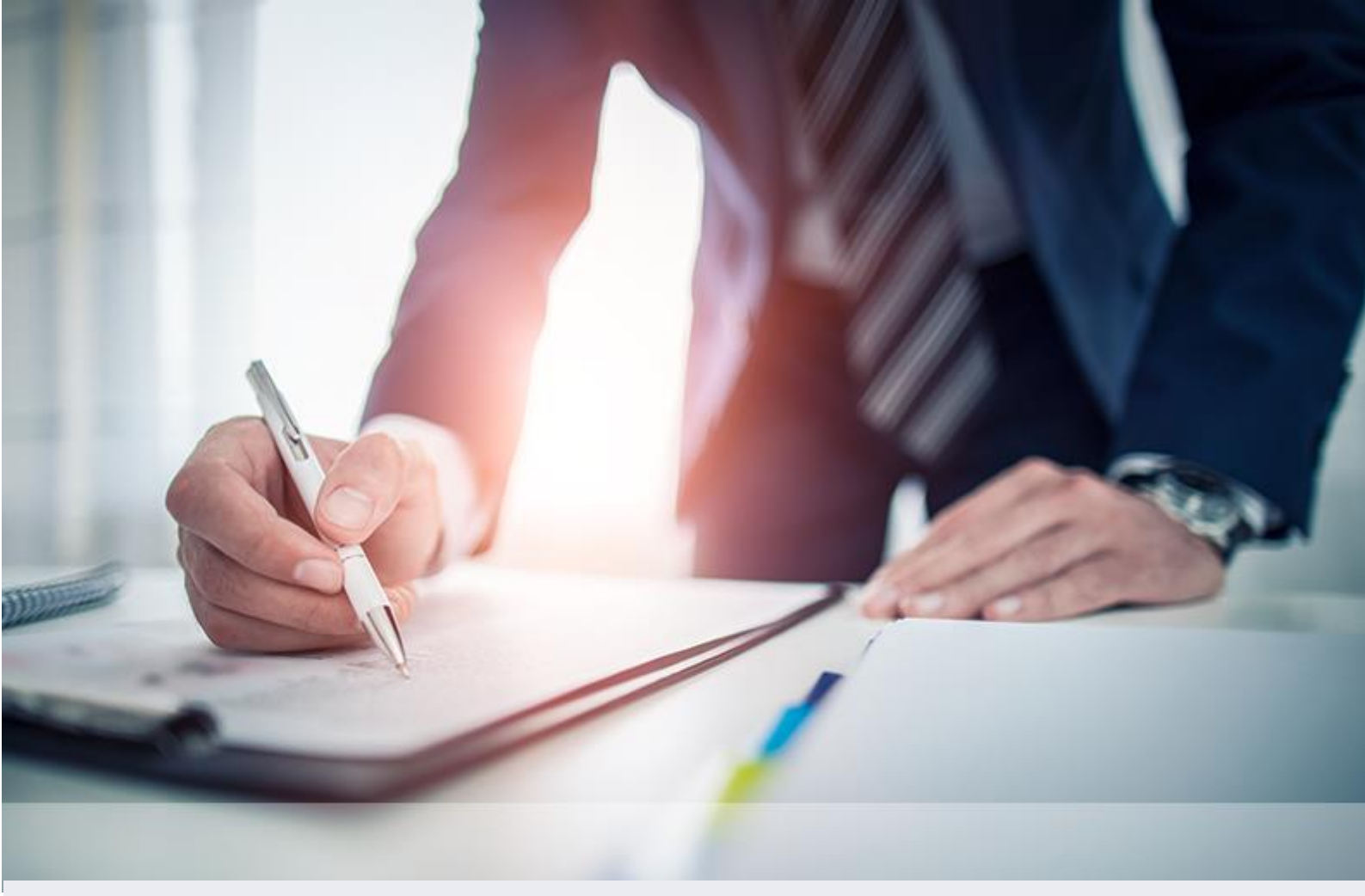
In general, caution is required if the DHCP server is not under your own control, for example in public WLANs or hotspots.

In privately operated networks, an attack would nevertheless be conceivable by attackers who operate a second DHCP server in the same network without being recognized.

Technically savvy users can detect the attack by analyzing the routing table on the client computer.

Further information

1. https://www.leviathansecurity.com/blog/tunnelvision
2. https://github.com/advisories/GHSA-jcv7-6v4q-4m7x



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Deutschland

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