Stellungnahme

Schwachstelle „Tunnelvision“ (CVE-2024-3661)

Stellungnahme zur Schwachstelle „Tunnelvision“ (CVE-2024-3661)

Die von der "Leviathan Security Group" entdeckte Schwachstelle namens „Tunnelvision“ (CVE-2024-3661) zielt auf via VPN angebundene Remotearbeitsplätze bzw. -netze ab. Der Angriff erfolgt hierbei nicht direkt auf einen vorhandenen VPN-Client, sondern auf das Routing im jeweiligen Betriebssystem.
Durch die implementierungs- bzw. herstellerunabhängige Natur des Angriffs sind auch sämtliche Remote-Arbeitsplätze mit NCP-VPN-Clients betroffen, ausgenommen auf der Android-Plattform.

Angriffsmethode

Der Angreifer imitiert im Netzwerk des Remote-Anwenders einen DHCP-Server, der mit Hilfe der DHCP-Option 121 die Routingtabelle auf dem Anwenderrechner manipuliert. Ziel dieser Manipulation ist, dass Daten nicht über die Standardroute durch den VPN-Tunnel versendet werden, sondern am VPN-Tunnel vorbei geleitet werden.
Verbindungen, die innerhalb des VPN-Tunnels Ende-zu-Ende-verschlüsselt sind, wie gewöhnliche Website-Aufrufe über HTTPS bzw. TLS, können weiterhin nicht entschlüsselt werden. Kommunikation, die unverschlüsselt durch den VPN-Tunnel gesendet wird, könnte durch den Angriff abgefangen werden. Außerdem können Metadaten und Informationen über das interne VPN-Netzwerk abfließen, wie z.B. IP-Adressen.
Verschleiernde bzw. anonymisierende VPNs, wie sie kommerziell in großer Zahl angeboten werden, werden durch den Angriff außer Funktion gesetzt; die Kommunikation findet dann nicht mehr durch den VPN-Tunnel statt.
VPNs, die in Enterprise-Umgebungen eingesetzt werden, um auf private Rechnernetze zuzugreifen, wie es häufig bei Kunden von NCP der Fall ist, sind von dem Angriff weniger stark betroffen, da die Verbindungsziele nicht über das Internet (außerhalb des VPN-Tunnels) erreichbar sind; in diesem Fall könnten die Angreifer nur die initiale Nachricht für den Verbindungsaufbau abgreifen, weitere Kommunikation mit dem privaten Rechnernetz würde nicht stattfinden.

Gegenmaßnahmen

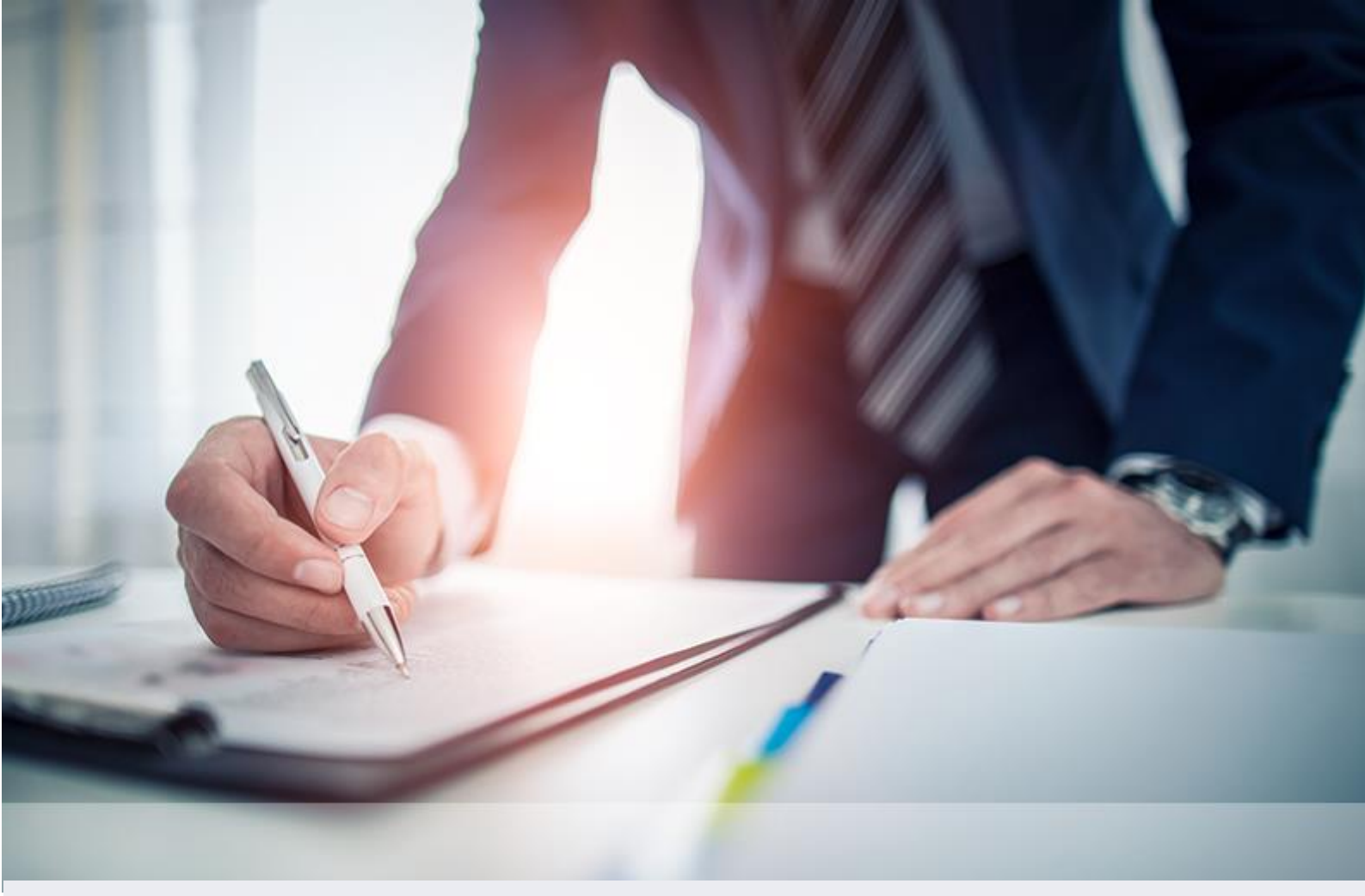
Maßnahmen, um den Angriff abzuwehren bzw. zu verhindern:

- Deaktivierung von DHCP und Verwendung von fest vergebenen IP-Adressen
- Kein „Split Tunneling“ verwenden, wenn verfügbar „lokale Netze im Tunnel weiterleiten“, und Nutzung einer Firewall, um ausschließlich VPN-Traffic zuzulassen (bitte die Hinweise „Problems with Firewall Rule Mitigations“ in 1) beachten!)

Grundsätzlich ist insbesondere dann Vorsicht geboten, wenn der DHCP-Server nicht unter der eigenen Kontrolle steht, beispielsweise in öffentlichen WLANs oder Hotspots.
In privat betriebenen Netzen wäre ein Angriff dennoch denkbar durch Angreifer, die unerkannt einen zweiten DHCP-Server im selben Netz betreiben.
Durch technisch versierte Nutzer kann der Angriff durch Analyse der Routingtabelle auf dem Clientrechner erkannt werden.

Weiterführende Informationen

1. https://www.leviathansecurity.com/blog/tunnelvision
2. https://github.com/advisories/GHSA-jcv7-6v4q-4m7x
3. https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2024-1047



NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg
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