Stellungnahme zu den TunnelCrack Schwachstellen (VU#563667)

Auf der Website tunnelcrack.mathyvanhoef.com werden zwei allgemeine Klassen von Angriffen gegen VPN-Clients beschrieben, mit denen ein Angreifer bewirken kann, dass Netzwerk-Datenverkehr vom Benutzerrechner (PC, Notebook, Smartphone), welcher eigentlich für den VPN-Tunnel bestimmt ist, unzulässigerweise am VPN-Tunnel vorbei unverschlüsselt in das lokale bzw. öffentliche Netz gelangt.

Diese Angriffe richten sich gegen die bei VPN-Clients gängige Vorgehensweise, dass anhand von sogenannten Routing-Tabellen des Betriebssystems festgelegt wird, welcher Datenverkehr durch den VPN-Tunnel geleitet werden soll und welcher nicht. Selbst ohne Split-Tunneling-Konfiguration gibt es typischerweise zwei Ausnahmen für bestimmte Arten von Netzwerkverkehr, die nicht in den Tunnel geleitet werden:

- Netzwerkverkehr, welcher für das lokale Netzwerk bestimmt ist (LocalNet-Ausnahme)
- Netzwerkverkehr, welcher für den VPN-Server bestimmt ist (ServerIP-Ausnahme)

Bei den LocalNet-Ausnahmen handelt es sich um ein Komfort-Feature um z.B. sicherzustellen, dass man im Homeoffice auch bei aktivem VPN-Tunnel weiterhin den Drucker im lokalen Netzwerk verwenden kann.

Die ServerIP-Ausnahmen sind erforderlich, um zu gewährleisten, dass bereits verschlüsselter VPN-Netzwerkverkehr direkt zum VPN-Server geschickt und nicht erneut in den VPN-Tunnel geschickt wird, was zu einer Endlosschleife führen würde.

Entsprechend den beiden Ausnahme-Typen unterscheidet man zwischen LocalNet- und ServerIP-Angriffen.

LocalNet-Angriffe

Um einen LocalNet-Angriff durchführen zu können, benötigt der Angreifer die Kontrolle über das lokale Netzwerk. Typischerweise kann dies geschehen, wenn sich der Anwender mit einem WLAN-Accesspoint verbindet, welcher unter der Kontrolle des Angreifers steht.

Das Ziel des Angriffs besteht darin, den Netzwerkdatenverkehr des Clients zu einem bestimmten Zielrechner umzuleiten, so dass die Verbindung nicht durch den VPN-Tunnel, sondern unverschlüsselt am Tunnel vorbei erfolgt. Wenn sich der Rechner mit dem Accesspoint verbindet, bekommt er per DHCP eine Adresse und Netzmaske für sein lokales Subnetz zugewiesen. Der Angreifer wählt den Adressbereich so, dass sich Client und Zielrechner im gleichen Subnetz befinden und damit die LocalNet-Ausnahme greift.

Je nachdem, welchen Erfolg der Angreifer mit dieser Attacke hat, kann man zwei Fälle unterscheiden.

LocalNet-Angriff mit Datenleck (CVE-2023-36672)

Dies ist die Hauptvariante, bei der der Angreifer sein Ziel in vollem Umfang erreicht: Die LocalNet-Ausnahme des VPN-Clients bewirkt, dass der gesamte Datenverkehr des Benutzers zum Zielrechner am schützenden VPN-Tunnel vorbei zum Accesspoint des Angreifers geschickt wird.

Anmerkung: *Sofern die Kommunikation mit dem Server über ein geschütztes Protokoll (z.B. TLS, SSH) erfolgt, gelangen die Daten nicht komplett unverschlüsselt zum Angreifer. Trotzdem erhält er Zugriff auf wertvolle Meta-Informationen wie z.B. IP-Adressen der beteiligten Rechner oder verwendete Kommunikations-Protokolle.*

Geschäftsführer: Ralf Koenzen | Aufsichtsratsvorsitz: Bosco Novák | Amtsgericht Aachen HRB 16976 | USt-IdNr. DE311887270

LocalNet-Angriff mit Blockierung der Daten (CVE-2023-35838)

In dieser Nebenvariante werden die Daten nicht abgeleitet, sondern vom VPN-Client oder einer Firewall geblockt werden.

Der Angreifer kann also nicht den Datenverkehr zu dem Zielrechner belauschen, ihm bleibt jedoch immerhin die Möglichkeit den Datenverkehr zu diesem Zielrechner unbemerkt zu unterbinden. Daher wird auch dieser Fall von den Sicherheitsforschern als (weniger schwerwiegende) Schwachstelle angesehen. Als Beispiel nennen sie eine Überwachungskamera, die sich nicht mit ihrem Server verbinden kann. (Vergleichbare Szenarien wären das z.B. Unterbinden von automatischen Software-Updates oder Updates von Signaturdateien von Viren-Scannern.)

Anmerkung: *Das Blockieren der Daten erfolgt bei manchen VPN-Clients, weil die LocalNet-Ausnahme nur dann angewandt wird, wenn das lokale Netzwerk einen privaten IP-Adressbereich gemäß RFC 1918 zugewiesen bekommt. Diese Maßnahme bietet jedoch nur eingeschränkten Schutz gegen Datenlecks und wirkt nur, wenn es sich bei dem Zielrechner um einen Server mit einer öffentlichen IP-Adresse und nicht um einen Server im Intranet der Firma handelt.*

Gegenmaßnahmen gegen LocalNet-Angriffe

LANCOM Systems empfiehlt für seine Advanced VPN Clients die folgenden Maßnahmen:

LANCOM Advanced VPN Client für Windows

Beim LANCOM Advanced VPN Client für Window kann der LocalNet-Angriff mit der Konfigurationsoption „Full Local Network Enclosure Mode“ / „Auch lokale Netze im Tunnel weiterleiten“ verhindert werden. Dadurch werden grundsätzlich alle Daten durch den VPN-Tunnel versendet.

Alternativ kann auch die im LANCOM Advanced VPN Client integrierte Firewall so konfiguriert werden, dass ausschließlich VPN-Datenverkehr (Firewall-Option „IPsec-Protokoll zulassen“) zugelassen ist, mit dedizierten Ausnahmen für z.B. den Netzwerkdrucker im Homeoffice. Zu beachten ist, dass diese Firewall-Regeln zum unbemerkten Blockieren wichtiger Daten führen können (CVE-2023-35838), hierfür sind separate Gegenmaßnahmen zu ergreifen.

LANCOM Advanced VPN Client für macOS

Beim LANCOM Advanced VPN Client für macOS kann der LocalNet-Angriff mit der Konfigurationsoption „Full Local Network Enclosure Mode“ nur eingeschränkt verhindert werden. Datenverkehr, der an das Standard-Gateway adressiert ist, wird nicht in den VPN-Tunnel geleitet.

Alternativ kann auch die Firewall eines Drittanbieters so konfiguriert werden, dass ausschließlich VPN-Datenverkehr zugelassen ist, mit dedizierten Ausnahmen für z.B. den Netzwerkdrucker im Homeoffice. Zu beachten ist, dass diese Firewall-Regeln zum unbemerkten Blockieren wichtiger Daten führen können (CVE-2023-35838), hierfür sind separate Gegenmaßnahmen zu ergreifen.

Geschäftsführer: Ralf Koenzen | Aufsichtsratsvorsitz: Bosco Novák | Amtsgericht Aachen HRB 16976 | USt-IdNr. DE311887270

ServerIP-Angriffe

Auch hier besteht das Ziel des Angriffs darin, den Netzwerkdatenverkehr des Clients zu einem bestimmten Zielrechner umzuleiten, so dass die Verbindung nicht durch den VPN-Tunnel, sondern unverschlüsselt am Tunnel vorbei erfolgt. Hierfür wird die ServerIP-Ausnahme genutzt.

Im Wesentlichen gibt es zwei Varianten, mit unterschiedlich Auswirkungen.

Anmerkung: *Der Einfachheit halber gehen wir auch im Folgenden davon aus, dass der Angreifer den Accesspoint kontrolliert. Die Voraussetzungen für den Angriff lassen sich im Fall des ServerIP-Angriffs jedoch noch weiter abschwächen, siehe Abschnitt 3: Threat Model der Original-Publikation.*

ServerIP-Angriff mit Datenleck zu beliebigen IP-Adressen (CVE-2023-36673)

Die Hauptvariante setzt zusätzlich voraus, dass der Angreifer die IP-Adresse manipulieren kann, mit der sich der VPN-Client zum VPN-Server verbinden möchte. Dies ist zum Beispiel der Fall, wenn der VPN-Client die IP-Adresse des VPN-Servers durch eine ungesicherte DNS-Anfrage ermittelt. In diesem Fall hat der Angreifer die Möglichkeit, durch DNS-Spoofing zu erreichen, dass die IP-Adresse des VPN-Servers mit der IP-Adresse des zu überwachenden Zielrechners übereinstimmt.

Damit eine VPN-Verbindung trotz der Umleitung zustande kommt, leitet der Angreifer den VPN-Datenverkehr vom Benutzerrechner an das echte VPN-Server weiter. Sobald der Tunnel aufgebaut ist, bewirkt die ServerIP-Ausnahme, dass der gesamte Datenverkehr des Benutzers zum Zielrechner am schützenden VPN-Tunnel vorbei zum Accesspoint des Angreifers geschickt wird. Der Benutzer bemerkt davon in der Regel nichts, da der VPN-Tunnel steht und alle Netzwerkverbindungen bis auf die zum Zielrechner normal durch den Tunnel geleitet werden.

ServerIP-Angriff mit Datenleck zur IP-Adresse des VPN-Servers (CVE-2023-36671)

Wenn der Angreifer die IP-Adresse des VPN-Servers nicht manipulieren kann, z.B. weil sie in der VPN-Konfiguration explizit eingetragen ist, hat er nur geringe Möglichkeiten die ServerIP-Ausnahme für ein Datenleck zu nutzen, da außer dem VPN-Datenverkehr normalerweise keine Netzwerk-Kommunikation direkt zum VPN-Server erfolgt.

Dem Angreifer bleibt jedoch die Möglichkeit, die öffentliche IP-Adresse des Benutzers in Erfahrung zu bringen. Dieser sogenannte Deanonymisierungs-Angriff stellt vor allem dann ein Sicherheitsrisiko dar, wenn das VPN vom Anwender zum Schutz der Anonymität und zur Zensurumgehung genutzt wird, und ist daher von untergeordneter Bedeutung für den typischen Anwendungsfall von LANCOM VPN-Produkten, bei dem die VPN-Verbindung vorrangig dem sicheren Zugriff auf firmeninterne Ressourcen dient. Die Details dieses Angriffs können in Abschnitt 4.2.1 der Originalpublikation nachgelesen werden.

ServerIP-Angriff mit Blockierung der Daten

Dieser Fall ist analog zu CVE-2023-35838, bietet dem Angreifer jedoch noch weniger Möglichkeiten ihn sinnvoll auszunutzen. Daher wurde von den Autoren keine separate CVE-Nummer vergeben.

Gegenmaßnahmen gegen ServerIP-Angriffe

LANCOM Systems empfiehlt für seine Advanced VPN Clients die folgenden Maßnahmen:

LANCOM Advanced VPN Client für Windows

Das Datenleck zu beliebigen IP-Adressen (CVE-2023-36673) kann dadurch verhindert werden, dass man in der VPN-Konfiguration den VPN-Server nicht mit einem Domainnamen, sondern mit einer IP-Adresse konfiguriert. Eine Nutzung von authentisierten DNS-Varianten (DNSSEC) ist momentan noch nicht möglich.

Zusätzlich kann man die integrierte Firewall des Windows-Clients so konfigurieren, dass außerhalb des VPN-Tunnels ausschließlich die für die VPN-Verbindung erforderlichen Protokolle zugelassen werden. Dies geschieht, indem man in der Firewall die Option „IPsec-Protokoll zulassen“ aktiviert und keine weiteren Firewall-Regeln definiert.

LANCOM Advanced VPN Client für macOS

Das Datenleck zu beliebigen IP-Adressen (CVE-2023-36673) kann dadurch verhindert werden, dass man in der VPN-Konfiguration den VPN-Server nicht mit einem Domainnamen, sondern mit einer IP-Adresse konfiguriert. Eine Nutzung von authentisierten DNS-Varianten (DNSSEC) ist momentan noch nicht möglich.

Zusätzlich kann man die Firewall eines Drittanbieters so konfigurieren, dass außerhalb des VPN-Tunnels ausschließlich die für die VPN-Verbindung erforderlichen Protokolle zugelassen werden. Es handelt sich hierbei um die Protokolle ISAKMP (UDP Port 500) und IPsec NAT-T (UDP Port 4500).

Quelle:

NCP engineering GmbH

Dombühler Str. 2

90449 Nürnberg

Deutschland

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