bintec Secure IPSec Client

Release Notes V. 6.14

1 Voraussetzungen

Microsoft Windows Betriebssysteme - Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit
- Windows 10, 64 Bit

Beachten Sie, dass die Version 6 des Secure Client eine neue Lizenz erfordert, auch wenn Sie von einer früheren Version upgraden.

2 Neue Leistungsmerkmale und Erweiterungen

- **Neue Option: „DNS Domains im Tunnel auflösen“**
  Die Split-DNS-Funktionalität lässt sich mit Hilfe der neuen Option „DNS Domains im Tunnel auflösen“ / „DNS domains to be resolved in the tunnel“ konfigurieren. Dabei werden im Falle von konfiguriertem Split Tunneling die DNS-Requests der konfigurierten Domains in den VPN-Tunnel gesendet. Alle anderen DNS-Requests gehen am VPN-Tunnel vorbei.
- **Unterstützung des RFC 7296**
  Der VPN-Client unterstützt nun RFC 7296 zur Verteilung von Split Tunneling-Konfigurationen seitens des VPN-Gateways.

3 Verbesserungen / Fehlerbehebungen

- **Neue Rechtestruktur innerhalb C:\ProgramData\NCP**
  Ein Benutzer hatte innerhalb des Verzeichnisses C:\ProgramData\NCP\ Schreibrechte. Diese wurden auf ein Minimum begrenzt. Beispielsweise kann ein Benutzer nun keine CA-Zertifikate mehr im dafür vorgesehenen Verzeichnis ablegen. Ebenso wurde die Verzeichnis- und Rechtestruktur so umgebaut, dass keine Anwendung im User- und System-Kontext in das gleiche Verzeichnis schreibt. Das Problem wurde behoben.
- **Verbesserungen beim serverseitig konfigurierten Split-DNS**
- **Automatische Windows-Anmeldung**
  Wurde innerhalb der Logon-Optionen die Option „Automatisch mit konfigurierten Anmeldedaten durchführen“ ausgewählt, so funktionierte die Windows-Anmeldung nicht. Ebenso gab es ein Problem in Verbindung mit 2-Faktor-Authentisierung via TOTP. Dieses Problem wurde behoben.
- **Problembehebung bei Seamleass Roaming und IPv6-Zieladressen**
- **VPN-Benutzername aus Cache**
  Nach dem Update einer Vorversion wurde u.U. der zwischengespeicherte VPN-Benutzername im Anmeldedialog nicht korrekt angezeigt. Dieses Problem wurde behoben.
- **Falsche Statusanzeige nach Profilwechsel**

Nach einem Profilwechsel von einem zertifikatsbasierten Profil mit erfolgreicher PIN-Eingabe auf ein Profil mit Pre-Shared-Key wurde die eingegebene PIN nicht gelöscht und das PIN-Icon nicht aus der Client-GUI entfernt. Dieses Problem wurde behoben.

- **PKI-Error beim Profilwechsel**
  Beim Profilwechsel von einem zertifikatsbasierten Profil mit *.p12-Datei auf ein Profil mit Smart-Card-Reader wurde ein PKI-Error angezeigt. Dieses Problem wurde behoben.
- **Update auf zlib Version 1.2.12**
  Die im VPN-Client verwendete zlib-Version wurde auf 1.2.12 angehoben. Damit wurde die zlib-Sicherheitslücke [CVE-2018-25032] geschlossen.
- **OpenSSL Sicherheitspatch**
  Die Sicherheitslücken [CVE-2022-0778] und [CVE-2020-1971] wurden in OpenSSL behoben.
- **Umstellung auf TLS 1.2**
- **Die TLS-Versionen 1.0 und 1.1 werden mit dieser Clientversion nicht mehr unterstützt.**
- **Update auf cURL-Library 7.84.0**
  Die im VPN-Client verwendete cURL-Version wurde auf 7.84.0 angehoben. Damit wurden die cURL-Sicherheitslücken [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207] und [CVE-2022-32208] geschlossen.
- **Die Kompatibilität zu Fremdgateways in Verbindung mit 2-Faktor-Authentisierung / Tokeneingabe wurde verbessert**
- **Falsche Statusanzeige: Chipkarte**
  Unter bestimmten Umständen wurde bei einem Profil mit 2-Faktor-Authentisierung fälschlicherweise ein Chipkartensymbol angezeigt. Beim Wechsel auf ein Profil mit Chipkarte wurde eine Fehlermeldung angezeigt, dass die Chipkarte nicht richtig initialisiert sei. Dieses Problem wurde behoben.
- **Problembehebung nach Änderung der DNS-Einträge in der VPN Bypass-Konfiguration**
- **Problembehebung beim Aufruf der HotSpot-Anmeldung**
  Die HotSpot-Anmeldung wurde nicht korrekt aufgerufen, wenn die Autostart-Option „Icon im System Tray“ ausgewählt war. Dieses Problem wurde behoben.
- **Problembehebung einer fälschlicherweise angezeigten PIN-Abfrage**
  Bei der Verwendung des CSP-Benutzerzertifikatsspeichers wurde i.A. fälschlicherweise eine PIN abgefragt. Dieses Problem wurde behoben. Ebenso wurde die Option zur PIN-Abfrage im Falle des CSP-Benutzerzertifikatsspeichers im Client Plug-in entfernt.
- **Verbesserung der Kompatibilität zu Fremdgateways bei der Adressierung via IPv6**
- **PAP/CHAP-Fehler beim Verbindungsaufbau**
  Unter bestimmten Umständen zeigt der VPN-Client beim IKEv2-Verbindungsaufbau einen PAP/CHAP-Fehler an. Dieser lässt sich durch den Anwender durch Öffnen des VPN-Profils und Bestätigen mit „Ok“ beheben. Dieses Problem wurde behoben.
- **Überarbeitung der Funktion „Verbindungsaufbau vor Windows-Anmeldung“**
  Um einer möglichen Priviledge Escalation vorzubeugen, wurde die Funktion „Verbindungsaufbau vor Windows-Anmeldung“ überarbeitet. Hierbei konnte ein Standard-Benutzer, sofern diese Funktion nicht über die Konfigurationssperren deaktiviert war, sich Administratorrechte, z.B. über eine konfigurierte CMD-Shell, erschleichen. Mit dieser Änderung können nur vom Administrator im Verzeichnis C:\ProgramData\NCP\SecureClient\scripts\ angelegte Batch-Dateien ausgewählt werden.
- **Verbesserung der Kompatibilität zu Juniper SRX-Gateways im Falle der ReKeying-Phase**
- **Unterstützung von RFC 8598**

In RFC 8598 ist die Weitergabe der Split-DNS-Konfiguration durch das VPN Gateway an den VPN Client definiert. Dieses RFC wird ab dieser Clientversion unterstützt.

- **Netzwerkverbindung nach Installation dauerhaft getrennt**
  Nach der Installation des Clients war die Netzwerkverbindung dauerhaft getrennt. Erst nach dem Reboot des Rechners war wieder eine Netzwerkkommunikation möglich. Dieses Problem wurde behoben.
- **Problem beim Importieren eines zuvor exportierten Profils**
  Der Import eines exportierten Profils in einen 13-er Client schlug fehl. Dieses Problem wurde behoben.
- **Allgemeine Verbesserungen beim INI- oder PCF-Datei-Import**
- **Verbesserung der Kompatibilität zu Fremdgateways hinsichtlich IP-Adresszuweisung**
  Wurde dem VPN Client während des Verbindungsaufbaus eine IP-Adresse, endend mit .255, zugewiesen, so war kein Routing durch den VPN-Tunnel möglich. Dieses Problem wurde behoben.
- **Problembehebung bei Online-Aktivierung, wenn Proxy verwendet und als DNS-Name konfiguriert ist**

4 Bekannte Einschränkungen

- **Option: „Dialog für Verbindungsaufbau automatisch Öffnen“**
  Unter bestimmten Umständen funktioniert die Logon-Option „Dialog für Verbindungsaufbau automatisch Öffnen“ nicht.
- **Applikationsbasierte VPN Bypass Konfiguration**
  Die Konfiguration eines DNS innerhalb der VPN Bypass Konfiguration macht eine darin enthaltene applikationsbasierte Regel unwirksam.
- **PIN-Menüeinträge**
  Bei der Verwendung von Hardware-Zertifikaten sind die PIN-Menüeinträge „PIN eingeben/zurücksetzen/ändern“ / „Enter/Reset/Change PIN“ ohne Funktion, jedoch fälschlicherweise auswählbar.
- **Seamless Roaming**
  Unter bestimmten Umständen verbleibt der VPN-Tunnelstatus beim Wechseln von WLAN auf LAN auf „Tunnel logisch halten“ und eine funktionale Verbindung über LAN wird nicht aufgebaut. Dies muss durch manuelles Trennen und Verbinden geschehen.
- **Home Zone und IPv6**
  Ist in den Firewall-Einstellungen des VPN-Clients die vordefinierte Home Zone-Regel aktiv, so werden im definierten Home Zone-Netzwerk ausgehende IPv6-Pakete in das lokale Netzwerk verworfen.