bintec Secure IPSec Client Version 4.14 Build r42039: Verbesserungen und Fehlerbehebungen

- **Prüfung eines Verbindungsmediums auf Internetverfügbarkeit:**
  Die Prüfung auf Internetverfügbarkeit mittels periodisch abgesetzter Pings auf 8.8.8.8 wurde auf maximal vier Pings begrenzt.

- **Optimierungen im Bereich HotSpot-Anmeldung:**
  Es wurden verschiedene Optimierungen im Bereich der HotSpot-Anmeldung vorgenommen, insbesondere bei der Verwendung von Seamless Roaming in den Profileinstellungen.

- **Credential Provider – Sicherheitslücke:**
  Bei der Verwendung des NCP Credential Providers konnte ein Anwender über das Log-Fenster und den darin enthaltenen **Öffne Datei**-Button Zugriff auf den Windows-Explorer bekommen. Darüber war es möglich sich administrative Rechte in der PowerShell zu verschaffen. Dieses Problem ist behoben.

- **Deinstallation des Clients:**
  Unter bestimmten Umständen konnte es vorkommen, dass der Filtertreiber des VPN Clients nicht korrekt deinstalliert wurde. Dieses Problem ist behoben.

- **Software-Update über andere NCP-OEM Clients ist nicht gesperrt:**
  Beim Durchführen eines Client Updates muss die OEM-Variante des Clients übereinstimmen. Der Versuch eines Updates mit einer fremden Version muss für diesen Fall verriegelt sein. Dies ist nun gewährleistet.

- **Adresszuweisung auf NCP Netzwerkadapter:**
  Bei Verwendung eines Juniper-Gateways konnte unter bestimmten Umständen dem NCP-Netzwerkadapter keine Netzwerkadresse zugewiesen werden. Dieses Problem ist nun behoben.

- **Das Handling verfügbarer Verbindungsmedien nach dem Aufwachen aus dem Sleep-Mode wurde verbessert.**

- **IKEv1 / Aggressive Mode:**
  Bei der Verwendung von IKEv1 mit Aggressive Mode konnten in Verbindung mit einer automatischen IKE-Richtlinie Probleme auftreten. Dieser Fehler ist behoben.