bintec Secure IPSec Client Version 4.14 Build r42039: Improvements and Bug Fixes

- **Checking a connection medium for Internet availability:**
  Testing for Internet availability by means of periodically dropped pings to 8.8.8.8 has been limited to a maximum of four pings.

- **Optimizations of the hotspot registration:**
  Various optimizations have been made in the hotspot logon application, especially when using Seamless Roaming in the profile settings.

- **Credential Provider – Vulnerability:**
  When using the NCP Credential Provider, a user could access the Windows Explorer via the log window and the **Open File** button contained therein. It was also possible to gain administrative rights in PowerShell. This problem is resolved.

- **Uninstall the client:**
  Under certain circumstances, the filter driver of the VPN client was not be uninstalled correctly. This problem is resolved.

- **Software update via other NCP OEM clients is not blocked:**
  When performing a client update, the OEM variant of the client must match. An attempt to update must be locked for this case. This is now enforced.

- **Address assignment to NCP network adapter:**
  When using a Juniper gateway, under certain circumstances, the NCP network adapter could not be assigned a network address. This problem is now fixed.

- **The handling of available connection media after waking up from sleep mode has been improved.**

- **IKEv1 / Aggressive Mode:**
  Using IKEv1 with Aggressive Mode could cause problems with an automatic IKE policy. This error is fixed.