bintec Secure IPSec Client

Release Notes V. 6.11

1 Requirements

Microsoft Windows Operating Systems - The following Microsoft Windows operating systems are supported with this release:

- Windows 11, 64 bit
- Windows 10, 64 bit

Note that version 6 of Secure Client requires a new license, even if you are upgrading from an earlier version.

2 New features and enhancements

- **New option: "Resolve DNS domains in the tunnel".**
  The split DNS functionality can be configured using the new option "Resolve DNS domains in the tunnel" / "DNS domains to be resolved in the tunnel". In the case of configured split tunneling, the DNS requests of the configured domains are sent into the VPN tunnel. All other DNS requests bypass the VPN tunnel.
- **RFC 7296 support**
  The VPN client now supports RFC 7296 for distributing split tunneling configurations on the part of the VPN gateway.

3 Improvements / Bug fixes

- **New rights structure within C:\ProgramData\NCP\.**
  A user had write permissions within the directory C:\ProgramData\NCP\. These have been limited to a minimum. For example, a user can now no longer store CA certificates in the designated directory. Likewise, the directory and permissions structure has been rebuilt so that no application in the user and system context writes to the same directory. The problem has been fixed.
- **Improvements in server-side configured split DNS**
- **Automatic Windows logon**
  If the option "Perform automatically with configured credentials" was selected within the logon options, the Windows logon did not work. Likewise, there was a problem in connection with 2-factor authentication via TOTP. This problem has been fixed.
- **Troubleshooting Seamleass Roaming and IPv6 Destination Addresses**
- **VPN username from cache**
  After updating a previous version, the cached VPN username was sometimes not displayed correctly in the login dialog. This problem has been fixed.
- **Incorrect status display after profile change**
  After a profile change from a certificate-based profile with successful PIN entry to a profile with pre-shared key, the entered PIN was not deleted and the PIN icon was not removed from the client GUI. This issue has been fixed.

- **PKI error during profile change**
  When switching profiles from a certificate-based profile with *.p12 file to a profile with SmartCard reader, a PKI error was displayed. This problem has been fixed.
- **Update to zlib version 1.2.12**
  The zlib version used in the VPN client has been raised to 1.2.12. This closed the zlib vulnerability [CVE-2018-25032].
- **OpenSSL Security Patch**
  The vulnerabilities [CVE-2022-0778] and [CVE-2020-1971] have been fixed in OpenSSL.
- **Switching to TLS 1.2**
  TLS versions 1.0 and 1.1 are no longer supported with this client version.
- **Update to cURL library 7.84.0**
  The cURL version used in the VPN client has been upgraded to 7.84.0. This closed the cURL vulnerabilities [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207], and [CVE-2022-32208].
- **Compatibility with third-party gateways in conjunction with 2-factor authentication / token entry has been improved**
- **Incorrect status display: chip card**
  Under certain circumstances, a profile with 2-factor authentication incorrectly displayed a smart card icon. When switching to a profile with a smart card, an error message was displayed stating that the smart card was not initialized correctly. This problem has been fixed.
- **Troubleshooting after changing the DNS entries in the VPN bypass configuration**
- **Troubleshooting when calling the HotSpot login.**
  The HotSpot login was not invoked correctly when the autostart option "Icon in system tray" was selected. This problem has been fixed.
- **Troubleshooting an erroneously displayed PIN query.**
  When using the CSP user certificate store, a PIN was sometimes incorrectly prompted. This problem has been fixed. Likewise, the PIN query option in the case of the CSP user certificate store has been removed in the client plug-in.
- **Improved compatibility with third-party gateways when addressing via IPv6**
- **PAP/CHAP error during connection establishment**
  Under certain circumstances, the VPN client displays a PAP/CHAP error when establishing an IKEv2 connection. This can be resolved by the user by opening the VPN profile and confirming with "Ok". This problem has been fixed.
- **Revision of the "Connection establishment before Windows logon" function**
  In order to prevent a possible privilege escalation, the "Connection setup before Windows logon" function has been revised. In this case, a standard user, if this function was not deactivated via the configuration locks, could sneak administrator rights, e.g. via a configured CMD shell. With this change, only batch files created by the administrator in the C:\ProgramData\NCP\SecureClient\scripts\ directory can be selected.
- **Improve compatibility with Juniper SRX gateways in case of rekeying phase**
- **Support of RFC 8598**
  RFC 8598 defines the forwarding of the split DNS configuration by the VPN gateway to the VPN client. This RFC is supported as of this client version.
- **Network connection permanently disconnected after installation**
  After installing the client, the network connection was permanently disconnected. Only after rebooting the computer, network communication was possible again. This problem has been fixed.
- **Problem importing a previously exported profile**
  Importing an exported profile into a 13 client failed. This problem has been fixed.
- **General improvements for INI or PCF file import**
- **Improvement of compatibility to third-party gateways regarding IP address assignment.**
  If the VPN client was assigned an IP address ending with .255 during connection establishment, routing through the VPN tunnel was not possible. This problem has been fixed.

- **Troubleshooting online activation when proxy is used and configured as DNS name**

4 Known limitations

- **Option: "Automatically open dialog for connection establishment".**
  Under certain circumstances the logon option "Automatically open dialog for connection establishment" does not work.
- **Application-based VPN bypass configuration**
  Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.
- **PIN menu items**
  When using hardware certificates, the PIN menu items "Enter/Reset/Change PIN" / "Enter/Reset/Change PIN" have no function but can be selected incorrectly.
- **Seamless roaming**
  Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.
- **Home Zone and IPv6**
  If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.