Release Notes
bintec Secure IPSec Client
Version 4.13

Inhalt

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10 32/64 Bit (bis einschließlich Version 1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

1 Neue Leistungsmerkmale und Erweiterungen

1.1 Anpassung an Windows 10 Version 1809 - Treiberinstallation

Aufgrund Microsoft-interner Änderungen war es mit vorhergehenden Clients nicht möglich eine Installation auf Windows 10 Version 1809 durchzuführen. Dieses Problem wurde behoben.

2 Verbesserungen / Fehlerbehebungen

2.1 Erkennung des Friendly Detection Server

In Netzwerken mit Network Access Control und Wechsel des IP-Segments nach erfolgreicher Authentisierung, wurde die Erkennung des Friendly Net Detection Servers verbessert.

2.2 Performanceoptimierung des Datentransfers außerhalb des VPN-Tunnels

Optimierung des Client Updateprozesses im Falle eines Major-Updates

Die Erkennung eines Major-Updates innerhalb des MSI-Installationsprozesses wurde verbessert. Ebenso wurde ein Problem mit der Umgebungsvariable `NcpClntInstallPath` behoben, die unter Umständen nach dem Update des Clients gelöscht war.

2.3 Anzeige des VPN-Clients in der Taskleiste

Wird die Client-GUI geschlossen, so wird das entsprechende Icon nicht mehr in der Taskleiste angezeigt. Dieses Verhalten entspricht dem Verhalten der Clientversionen vor 11.0.

2.4 Diagnosedaten im Installationsverzeichnis

Im Falle der aktivierten Full trace-Funktion oder einer konfigurierten HotSpot-Erkennung wurden fälschlicherweise Diagnosedateien in das Installationsverzeichnis des Clients geschrieben. Dieser Fehler wurde behoben.

2.5 Verbesserung der Silent Installation

Unter bestimmten Umständen konnte das REBOOT Property während der Installation des Clients überschrieben werden. Dieses Problem ist nun behoben.

2.6 Verbesserung der Kompatibilität zu DHCP-Servern

Bei einem DHCP-Request ist die Angabe des Hostnamens zwar optional, jedoch kommen nicht alle DHCP-Server mit dem Weglassen des Hostnamens zurecht. Aus diesem Grunde wird ab dieser Release immer der Hostname mitgeschickt.

2.7 Verbesserung der Kompatibilität zu Fremdgateways

Innerhalb der IKE-Verhandlung wurde die Kompatibilität zu Fremd-Gateways verbessert.

2.8 Firewall-Einstellung: Ausnahme für VPN Path Finder

Wurde in den Firewall-Einstellungen die Option „IPsec-Protokoll (ESP, UDP 500) und VPN Path Finder (TCP 443) zulassen“ konfiguriert, so waren Ziele durch den VPN-Tunnel via HTTPS-Port 443 erreichbar obwohl dies durch keine weitere Firewall-Regel erlaubt war. Dieser Fehler wurde behoben.

2.9 Länge des Namens einer PKCS#11-Datei

Die Länge des Eingabefeldes in der PKI-Konfiguration des Clients für das PKCS#11 Modul wurde auf 255 Zeichen erhöht.

2.10 Nachladen von DLLs

Verbesserung des DLL-Ladevorganges zur Erhöhung der Sicherheit vor manipulierten DLLs.

2.11 Verbesserung der Updateprüfung

Bei der Prüfung des Clients auf die Verfügbarkeit neuer Versionen wurde die Sicherheit vor Manipulation erhöht.

3 Bekannte Einschränkungen

3.1 Demo-Benutzerzertifikate

Die **Demo-Benutzerzertifikate**, die mit bisherigen Client-Versionen installiert wurden, verlieren ihre Gültigkeit am 9. Oktober 2018. Damit werden existierende Test-Profile, z. B. zum DemoServer "vpntest.ncp-e.com", ab diesem Zeitpunkt nicht mehr funktionieren. Ab dieser Clientversion steht bei Neuinstallationen die automatische Einrichtung dieser Test-Profile mit Zertifikat nicht mehr zur Verfügung. Es existiert ausschließlich die Möglichkeit, Test-Profile mit der VPN-Konfiguration **Pre-shared key** zu erstellen.

Neue Zertifikate mit verlängerter Gültigkeit befinden sich nach der Installation im Unterverzeichnis *certs*. Bisher waren sie immer direkt im Installationsverzeichnis abgelegt.