

# Release-Notes

## Release 1.12.3 05-Jun-2023

Neue Funktionen:

- Die 450 MHz Engine Quectel EC200S-EN wird unterstützt.
- OpenVPN: neue Option für TLS-Encryption.
- Die im SSH Server installierten authorized\_keys werden in einer Liste angezeigt.

## Release 1.12.2 28-Nov-2022

- behebt bei SIM Karten welche eine statische IPv6 Adresse vom Provider bekommen können, das diese in einigen Fällen tatsächlich nicht statisch ist. Diese SIM Karten funktionieren z.Z. nicht im NDIS Mode der Paketdatenverbindung.
- Der DHCP-Server zeigt an wann die verliehene Adresse abläuft.

## Release 1.12.1 25-Aug-2022

Sicherheitskorrekturen:

- Update auf openssl-1.1.1q behebt CVE-2022-1292 und CVE-2022-2068.

## Release 1.12.0 07-Jun-2022

Sicherheitskorrekturen:

- Update auf openssl-1.1.1n behebt CVE-2022-0778.
- Update auf expat-2.4.7 behebt CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314 und CVE-2022-25315.
- Update auf openvpn-2.4.12 behebt CVE-2022-0547.
- Update auf zlib-1.2.12 behebt CVE-2018-25032.

## Release 1.11.20 14-Dez-2021

Neue Funktionen:

- IPsec: AEAD (Authenticated Encryption with Associated Data) implementiert. Im IKEv2 Mode kann jetzt die Klasse der "Authenticated Encryption Algorithms" ausgewählt werden. Hier sind "AES-128 GCM8" bis "AES-256 GCM16" Auswählbar.
- IPsec: bei den klassischen Algorithmen kann jetzt die "Pseudo Random Function" auch unabhängig vom Hash-Wert gewählt werden.

## Release 1.11.19 03-Nov-2021

Korrekturen:

- In Geräten mit Quectel Mobilfunk Engines wurde die SIM Karten Authentifizierung mit Benutzername und Passwort korrigiert.

## Release 1.11.18 02-Nov-2021

Sicherheitskorrekturen:

- IPsec: Korrektur behebt CVE-2021-41990 und CVE-2021-41991.

Neue Funktion:

- Zum E-mail versenden können jeweils bis zu 10 Empfänger angegeben werden. Weitere Empfänger können, getrennt durch ein Komma, in jeder Zeile angegeben werden.

**Release 1.11.17** 11-Okt-2021

Neue Funktion:

- Die unter "Device services/SNMP setup/Configuration" angegebenen System Informationen können über dem Auswahlnenü und auf der Login-Seite angezeigt werden.

**Release 1.11.16** 09-Sep-2021

Sicherheitskorrekturen:

- Update auf openssl-1.1.1l behebt CVE-2021-3711 und CVE-2021-3712.

Neue Funktionen:

- IPsec: Im Mode IKEv2 können bis zu 5 Netze (Traffic Selectors) für die lokale und/oder entfernte Adresse, gesetzt werden. Die optionale NAT Funktion wirkt dabei nur auf das erste Paar aus lokalem und entferntem Netz.
- Die Quectel Mobilfunk Engines können im Netzwerk-Mode betrieben werden (QMI/GobiNet).

**Release 1.11.15** 26-Jul-2021

Verbesserungen:

- Behebt ein Problem aufgrund mangelnder Entropy im Kernel, welcher zum Stillstand des Gerätes führen kann.

**Release 1.11.14** 21-Jul-2021

Verbesserungen:

- Die unter Roaming teilweise häufigen Wechsel des Providers nach dem Start der Mobilfunk-Engine werden abgewartet bevor die Paketdatenverbindung aufgebaut wird. Dies behebt Probleme bei Verwendung von 1NCE SIM-Karten (APN: iot.1nce.net).

**Release 1.11.13** 10-Mai-2021

Sicherheitskorrekturen:

- Update auf openssl-1.1.1k behebt CVE-2020-1971, CVE-2021-3449 und CVE-2021-3450.
- Update auf dnsmasq-2.85 behebt CVE-2020-25684 und CVE-2020-25686.
- Update auf openvpn-2.4.11 behebt CVE-2020-15078.

Neue Optionen:

- In OpenVPN Verbindungen kann die ab openvpn-2.4 mögliche option compress benutzt werden. Weiterhin kann die Cipher-Gruppe AES-xxx-GCM ausgewählt werden.

**Release 1.11.12** 16-Marz-2021

- Engine fix für 1&1 LTE SIM-Karte.

**Release 1.11.11** 04-Marz-2021

Verbesserungen:

- In den IPsec Verbindungen kann jetzt eine UDP Verkapselung erzwungen werden.

**Release 1.11.10** 10-Dec-2020

Sicherheitskorrekturen:

- Update auf openssl-1.1.1i behebt CVE-2020-1971.

Fehlerkorrektur:

- IPsec mit XAuth ist wieder Funktionsfähig. Die Web-GUI sorgt dafür das XAuth nur mit IKEv1 arbeiten kann.  
Da XAuth nur für IPv4 geeignet ist, sollte die Adressierung auf IPv4 beschränkt werden wenn als Gegenstelle eine URL verwendet wird.

#### **Release 1.11.9** 01-Dec-2020

Fehlerkorrektur:

- IPv6 kann wieder im Mobilfunknetz aktiviert werden, auch wenn vorher eine IPv4 only SIM zum Einsatz kam.

#### **Release 1.11.8** 10-Nov-2020

Verbesserungen:

- Für SIM Karten welche schon bei der Registrierung im LTE Netz entsprechende Zugangsdaten benötigen, kann über den neuen Menüpunkt 'Credentials usage' die Einstellung 'Registration and Package data' gewählt werden.

#### **Release 1.11.7** 19-Okt-2020

Fehlerkorrektur:

- In der Title-Anzeige der Webserver-Schlüssel fehlte die Schlüssellänge.

#### **Release 1.11.6** 14-Okt-2020

Verbesserungen:

- die zulässige Startzeit für IPsec verlängert auf 30s um einen vorzeitigen Timeout zu vermeiden. Ansonsten kann es bei grossen Schlüssellängen zu einem vorzeitigen Abbruch des IPsec Prozesses führen.
- Der PKCS#12-Zertifikatsimport unterstützt jetzt Schlüssel mit elliptischen Kurven.

#### **Release 1.11.5** 23-Sep-2020

Neue Features:

- Die Narrowband Engine Quectel BG96 wird unterstützt. Bei Verwendung von 1NCE.COM SIM-Karten (APN: iot.1nce.net) ist das Roaming auf 'Disabled' zu setzen.  
Band 8 muss eingeschaltet sein (normal B3/B8/B20).
- Die Huawei Engine 'ME909s-120 V2' wird erkannt.
- Telekom SIM Karten welche nur mit dem Protokoll IPv6 arbeiten, können benutzt werden.  
Services wie Connection-Check und DynDNS stehen aber nur für IPv4 zur Verfügung.
- Der OpenVPN Server unterstützt neben dem NET30-Mode jetzt auch SUBNET-Mode.

Verbesserungen:

- korrigierte Bandeinstellungen für Quectel EC21-E, EC25-E, EC21-EUX und EC25-EUX.

#### **Release 1.11.4** 05-Jun-2020

Sicherheitskorrekturen:

- Patch für PPPD, behebt CVE-2020-8597
- Update auf openssl-1.1.1g behebt CVE-2020-1967.

Verbesserungen:

- Unterstützung für ext3 formatierte Datenträger (USB-Stick und SD-Karte)
- Der IPsec-Status zeigt den verwendeten Port der Gegenseite an.
- Der OpenNTPd Client wird bei Protokollfehler nicht mehr beendet sondern neu gestartet.
- IPsec arbeitet jetzt auch mit IPv6 Gegenstellen zusammen.
- Benutze den APN in context#2 bei Quectel Engines um mit Vodafone CDA arbeiten zu können.

### **Release 1.11.3** 31-Jan-2020

Sicherheitskorrekturen:

- behebt CVE-2017-16544 in busybox.
- eine authentifizierte Befehlsinjektion mit Hilfe einer händisch modifizierten POST Anweisung wird jetzt verhindert.

Verbesserungen:

- Der IPsec Status zeigt an ob NAT-Traversal benutzt wird.
- Es können bis zu 3 NTP-Server konfiguriert werden.
- kürzere Zeit zum Herunterfahren der Quectel Engines EC21/25.
- der SNMP-Daemon wird jetzt im Hintergrund verzögert gestartet um ein 6 minütiges Hängenbleiben bei Hochlaufen des Gerätes zu vermeiden.

### **Release 1.11.2** 20-Dez-2019

Änderungen:

- neue Artikel-Nr. und Bezeichnung wenn eine LTE CAT 4 Engine benutzt wird.

### **Release 1.11.1** 8-Nov-2019

Neue Features bzw. Sicherheitsupdates:

- Verwendung von OpenSSL-1.1.1 mit Unterstützung für TLS-1.3.
- Webserver mit TLS-1.3
- OpenVPN mit TLS-1.3
- E-Mail senden mit TLS-1.3

Verbesserungen:

- Verwendung der Native Posix Thread Library (NPTL)
- schnellerer Start-/Stop und Verbindungs-auf/abbau bei IPsec aufgrund der NPTL.

### **Release 1.10.6** 13-Aug-2019

Bugfix:

- Die SMS Weiterleitung funktioniert wieder.

### **Release 1.10.5** 08-Aug-2019

Neue Features:

- Für den openvpn Verbindungsaufbau kann die Adressfamilie eingestellt werden.
- Für den openvpn Server kann die Adressfamilie eingestellt werden.
  - "auto" : dual-stack, IPv4 und IPv6
  - "IPv4" : nur IPv4
  - "IPv6" : nur IPv6
- Ein Firmwareupdate ist jetzt auch über ssh möglich.

### **Release 1.10.4** 10-Jul-2019

Bugfix:

- Die unnötige Einschränkung in den "IP and port forwarding" Regeln auf 10 fortlaufende Ports entfernt wenn Quell- und Zielbereich identisch sind.

### **Release 1.10.3** 19-Jun-2019

Bugfix:

- Statusabfrage der Eingänge via XML-Server wieder funktionsfähig.
- Der Webserver funktioniert jetzt auch mit Zertifikaten welche von einer CA unterschrieben wurden.

## **Release 1.10.2** 23-Mai-2019

### Bugfix:

- Das Admin Passwort kann nur geändert werden wenn das alte Passwort eingegeben wurde.

## **Release 1.10.1** 09-Mai-2019

### Neue Features:

- Auf der WAN Seite kann der IPv6 Dualstack Betrieb aktiviert werden.  
Die Huawei Engines sind in der Europa Ausführung allerdings nicht IPv6 fähig.  
Die Tests wurden mit der Quectel Engine EC25E durchgeführt, welche IPv6 unterstützt.
- OpenVPN ist jetzt voll IPv6 fähig.
- Die TLS-Versionen TLS-1.0 und TLS-1.1 können für den Web-Zugriff deaktiviert werden.

### Sicherheitskorrekturen:

- Update auf openssl-1.0.2r, behebt CVE-2019-1559

### Korrekturen:

- Das Gerät muss jetzt seltener einen Reboot aufgrund eines Fehlers im Mobilfunknetz durchführen.

## **Release 1.09.8** 19-Mrz-2019

### Neue Features:

- Die Ethernet-Ports 2,3,4 sind abschaltbar.

## **Release 1.09.7** 25-Jan-2019

### Neue Features:

- In den Einstellungen zum DHCP-Server kann der autoritative Modus Ein-/Ausgeschaltet werden.
- In Firewall und Portweiterleitungen kann jeder Eintrag Ein-/Ausgeschaltet werden.
- Webserver mit Zertifikatsimport.

### Sicherheitskorrekturen:

- Update auf openssl-1.0.2q, behebt CVE-2018-5407 und CVE-2018-0734.

### Korrekturen:

- Fehlermeldungen beim Zertifikatsimport verbessert.

## **Release 1.09.6** 04-Jun-2018

### Sicherheitskorrekturen:

- strongswan CVE-2018-10811, CVE-2018-5388
- expat

### Verbesserungen:

- strongswan IKEv1 Reauthentisierung verbessert.

## **Release 1.09.5** 25-Mai-2018

### Verbesserungen:

- IPsec mit Unterstützung für IKEv2.
- IPsec mit SHA-256/384/512 sowie Diffie-Hellman mit elliptischen Kurven.
- Globale IPsec Firewall um Denial-of-service Angriffe abzuwehren.

## **Release 1.08.10** 04-Dez-2017

### Verbesserungen:

- verkürzte Latenzen im Web-GUI.

### Bugfix:

- IPsec mit 1:1 NAT und gleichzeitiges Portforwarding beeinflussen sich nicht mehr gegenseitig.

## **Release 1.08.9**                      05-Okt-2017

### **Verbesserungen:**

- Anzeige der Lizenz zu jedem Softwarepaket.
- Ablage der Texte aller Open-Source Lizenzen und Versionsinformationen der dazugehörigen Pakete.
- Der http/https Zugriff kann nun mittels der "Web Server Firewall" kontrolliert werden

### **Sicherheitskorrekturen:**

- dnsmasq CVE-2017-14491, CVE-2017-14492 und CVE-2017-14493.

### **Bugfix:**

- OpenVPN Preshared Key Import in Windows-Format.

## **Release 1.08.7**                      07-Aug-2017

### **Sicherheitskorrekturen:**

- OpenVPN in Version 2.3.17 behebt die Sicherheitslücken CVE-2017-7521, CVE-2017-7479 und CVE-2017-7478.

## **Release 1.08.5-beta**                25-Apr-2017

### **Verbesserungen:**

- Die Überwachung der Mobilfunk-Engines verschärft. Sollte die Mobilfunk-Engine während des Betriebs einen ungeplanten Neustart durchführen, so wird dies jetzt sofort erkannt und alle daran angeknüpften Dienste beendet. Weiterhin wird bei den Huawei-Engines erkannt ob die Paketdatenverbindung durch das Providernetzwerk unterbrochen wird und ein Wiederaufbau eingeleitet.

### **Sicherheitskorrekturen:**

- Ein Zurücksetzen auf Werkseinstellungen durch Drücken des Reset-Knopfes für mehr als 5 Sek. löst unmittelbar einen Neustart des Gerätes aus. Noch während das Gerät neu startet wird die alte Konfiguration komplett entfernt und durch die Werkseinstellung ersetzt. Sollte dieser Löschvorgang durch Unterbrechen der Spannungsversorgung beendet werden dann wird beim nächsten Neustart der Vorgang wiederholt.

### **Sicherheitsrelevante Änderungen:**

- Der https Zugriff unterstützt nur noch sichere Verschlüsselungs-Methoden.
- Der SSH Zugriff ist nicht mehr mit CBC-Methoden möglich.

### **Neue Features:**

- IPsec mit 1:1 NAT Tabelle. Dazu müssen im ersten Schritt unter Settings der Wert für "Connection NAT" auf "Local 1:1-NAT" oder "Remote masquerading" und der Wert "NAT to local network" auf "0.0.0.0" gesetzt werden (Apply drücken). Dann erscheint neben dem Wert für "NAT to local network" ein Edit-Knopf. Hier kann jetzt die Tabelle für das lokale 1:1 NAT editiert werden.
- Der OpenVPN-Server ist jetzt immer freigeschaltet.
- Unter "Network security/General setup" kann der Zugriff aus dem lokalem Netzwerk auf DNS-Dienste unterbunden werden.
- Unter "System/System configuration" kann die Konfiguration und Verwendung von IPsec komplett ausgeschaltet werden.

## **Release 1.07.4-beta**                09-Jan-2017

- Erstausgabe