Read Me
System Software 9.1.5 Patch 1

Deutsch **Version 9.1.5 Patch 1 unserer Systemsoftware ist für die Geräte der Serien RXL, RS, R(T)xxx2 und WLAN verfügbar.**

Beachten Sie, dass nicht alle aufgeführten Änderungen für alle Geräte zutreffen. Durch ein Update profitieren Sie aber in jedem Fall von den allgemeinen Verbesserungen im Hinblick auf Stabilität und Leistung.

1.1 Behobene Fehler

1.1.1 WLAN - Blacklist-Einträge gelöscht

(ID 17975)

Wenn der WLAN Controller eine Liste der von der Blacklist zu löschenden Einträge übertrug, löschte der Access Point alle Einträge anstelle nur der übertragenen von seiner Liste.

Das Problem ist gelöst.

1.1.2 WLAN - Unverschlüsselter Datenverkehr

(ID 17973)

Wenn der WPA-Modus eines Drahtlosnetzwerkes im GUI geändert wurde, ohne dass das Netzwerk vor der Umstellung deaktiviert wurde, konnte es dazu kommen, dass im Anschluss Multicast-Datenverkehr unverschlüsselt gesendet wurde.

Das Problem ist gelöst.

1.1.3 WLAN - Anzeigefehler

(ID 17942)

Nach einem Neighbor-Scan wurde alle ggf. gefundenen Access Points mit einer Signalstärke von 0 dB angezeigt.

Das Problem ist gelöst.

1.1.4 WLAN Controller - Access Point blockiert

(ID 17937)

Es konnte dazu kommen, dass ein vom WLAN Controller administrierter Access Point nicht mehr reagierte, wenn für das Netzwerk kein 802.11n-Standard verwendet wurde.

Das Problem ist gelöst.

1.1.5 WLAN - Panic

(ID 17939)

Es konnte zu gelegentlichen Neustarts von Access Points kommen.

Das Problem ist gelöst.

1.1.6 SIF - Probleme mit Schnittstellen- / Adressgruppen

(ID 17951, 17952)

Wenn bei der Konfiguration der Stateful Inspection Firewall eine sehr große Anzahl an Schnittstellen- bzw. Adressgruppen erstellt wurde, konnte es zu Fehlern in der Behandlung der Alias-Einträge und zu auch Neustarts des Geräts kommen.

Das Problem ist gelöst.

1.2 Bekannte Probleme

1.2.1 WLAN - WEP bei mehreren VSS

(ID 17627)

Es können auf einem Radiomodul nicht mehrere Drahtlosnetzwerke mit WEP-Verschlüsselung verwendet werden.

WEP gilt als unsicher. Verwenden Sie daher ein anderes Sicherungsverfahren (z.B. WPA2 mit AES).

English **Version 9.1.5 Patch 1 of our system software is available for the RXL, RS, R(T)xxx2 and WLAN series.**

Note that not all changes described here need to apply to all of the products. In any case, an update will allow you to benefit from the general improvements in stability and performance.

1.1 Fixed errors

1.1.1 WLAN - Blacklist entries deleted

(ID 17975)

If the WLAN controller transmitted list of entries to be removed form the black-list, the access point deleted all of the entries from its list instead of only the transmitted ones.

The problem has been solved.

1.1.2 WLAN - Unencrypted data traffic

(ID 17973)

If the security mode of a wireless network was changed in the GUI without first deactivating the VSS, multicast data traffic could be sent unencrypted.

The problem has been solved.

1.1.3 WLAN - Display error

(ID 17942)

After a neighborhood scan, all discovered access points were displayed with a signal strength of 0 dB.

The problem has been solved.

1.1.4 WLAN Controller - Access point locked up

(ID 17937)

An access point that was managed by the WLAN controller could become unrespronsive when the wireless network did not use the 802.11 standard.

The problem has been solved.

1.1.5 WLAN - Panic

(ID 17939)

Access points could occasionally reboot.

The problem has been solved.

1.1.6 SIF - Problems with interface/address groups

(ID 17951, 17952)

If a large number of interface or address groups was created during the configuration of the Stateful Inspection Firewall, this could lead to errors in the handling of alias entries as well as to reboots.

The problem has been solved.

1.2 Known Issues

1.2.1 WLAN - WEP with multiple VSS

(ID 17627)

It is not possible to use more than one VSS with WEP encryption per radio module.

WEP is considered insecure. You should, therefore, use a different security protocol (e.g. WPA2 with AES).