Read Me
System Software 9.1.12 Patch 2 WIQ

Deutsch **Folgende Fehler sind in Systemsoftware 9.1.12 Patch 2 korrigiert worden:**

1.1 WLAN - Neustart

(ID 19496)

Wenn mehrere inaktive VSS auf jedem Radiomodul eines Geräts mit mehreren Radiomodulen identisch konfiguriert waren, konnte es bei der Aktivierung eines der VSS zu einem Neustart des Gerätes kommen.

1.2 WLAN - Automatische Kanalwahl unzuverlässig

(ID 18836)

Die automatische Kanalwahl arbeitete nicht völlig zuverlässig und wählte nicht unter allen Umständen den besten Kanal.

1.3 WLAN Controller - Fehler bei Mischinstallationen

(ID 19530)

In WLAN-Infrastrukturen, die mit dem WLAN Controller administriert werden und Access Points unterschiedlicher Typen enthalten, konnte es zu diversen Fehlern - von GUI-Fehlermeldungen bis hin zu nicht funktionsfähigen Access Points - kommen.

1.4 Hotspot - Speicherverlust

(ID 19274)

Es konnte nach mehrtägigem Betrieb des Hotspot Servers zu einem Speicherfresser kommen.

1.5 WLAN Controller - WTP nicht korrekt verwaltet

(ID 19324)

Es konnte vorkommen, dass der WLAN Controller einen Slave Access Point nur nach einem Neustart des Slaves korrekt verwaltete.

1.6 Überwachung - Fehlinterpretation

(ID 19313)

Bei der Überwachung des Zustands eines Hosts anhand seiner IP-Adresse (***Lokale Dienste*** > ***Überwachung***) wurde der Host dann immer als inaktiv interpretiert, wenn der für ***Erfolgreiche Versuche*** konfigurierte Wert größer war als der für ***Fehlgeschlagene Versuche*** konfigurierte, auch wenn der Host erreichbar war.

1.7 GUI - Hotspot Timeout

(ID 19290)

Es war nicht möglich, die Option Standard-Timeout bei Inaktivität durch Setzen des Wertes *0* im Menü ***Lokale Dienste*** > ***Hotspot-Gateway*** > ***Neu/Bearbeiten*** zu deaktivieren.

1.8 Scheduler - Unbeabsichtigte Ausführung

(ID 18745)

Obwohl der Scheduler dadurch deaktiviert wurde, dass das Schedule-Interval auf *0* gesetzt wurde, konnte es dazu kommen, dass konfigurierte Aktionen aufgrund anderer Auslöser ausgeführt wurden.

1.9 DynDNS - Authentifizierung schlug fehl

(ID 19748)

Es konnte vorkommen, das bei Verwendung von DynDNS die Authentifizierung fehlschlug, weil das Passwort abgeschnitten wurde.

1.10 SNMP-Browser - MIB-Tabelle ipsecPeerTable nicht änderbar

(ID 19222)

Im GUI in der ***ANSICHT*** *SNMP-Browser* konnten die Einträge in der MIB-Tabelle *ipsecPeerTable* nicht geändert werden.

1.11 WLAN - Wiederholte Stacktraces

(ID 19760)

Bei der Nutzung mehrerer Bridge Links konnte es vorkommen, dass mindestens ein Bridge-Link-Paar Stabilitätsprobleme und Stacktraces nach ungefähr zwei Tagen Laufzeit aufwies. Beim betroffenen Access Point trat vor dem Stacktrace ein Speicherüberlauf auf.

1.12 WLAN - Falsche Anzahl von Slaves

(ID n/a)

Mit der Einstellung ***BETRIEBSMODUS*** = *Bridge Link Client* war mehr als ein Slave aktiviert, obwohl in diesem Modus nur ein Slave unterstützt wird.

1.13 WLAN Controller - WTP funktionierte nicht korrekt

(ID 19553)

Wenn mehrere WTPs von einem WLAN Controller verwaltet wurden, konnte es vorkommen, dass nach dem Aus- und wieder Einschalten eines WTP sich ein anderer WTP in einem falschen Zustand befand.

1.14 Netzwerk - Drop-In

(ID 19484)

Bei Verwendung einer Drop-In-Gruppe kam es zu zwei oder drei Reboots pro Tag.

1.15 WLAN Controller - Scan-Vorgang startete nicht

(ID n/a)

Unter bestimmten Umständen konnte es vorkommen, dass ein Scan-Vorgang , der vom WLAN Controller angestoßen wurde, nicht startete.

1.16 WLAN - Frequenzband 5 GHz Outdoor nicht verfügbar

(ID 19696)

Wenn unter ***WIRELESS LAN*** > ***VERWALTUNG*** > ***GRUNDEINSTELLUNGEN*** die Option ***REGION*** = *France* gewählt war, war im Menü ***WIRELESS LAN*** > ***WLAN*** > ***EINSTELLUNGEN FUNKMODUL*** > ***BEARBEITEN*** die Einstellung ***FREQUENZBAND*** = *5 GHz Outdoor* nicht verfügbar.

1.17 WLAN Controller - Stacktrace

(ID 19698)

Wenn Slave Access Points von einem Wireless LAN Controller verwaltet wurden, konnte es vorkommen, dass bei einigen Access Points mehrmals ein Stacktrace auftrat.

1.18 WLAN - Panic

(ID 19678)

Bei Access Points im Slave-Modus konnte es vorkommen, dass mehrmals am Tag eine Panic auftrat.

English **The following errors have been corrected in system software 9.1.12 Patch 2:**

1.1 WLAN - Restart

(ID 19496)

If multiple inactive VSS were configured identically for each radio of a dual radio device, a restart could occur upon activating one of the VSS.

1.2 WLAN - Automatic channel selection inaccurate

(ID 18836)

Automatic channel selection was not entirely accurate and did not select the best possible channel under all circumstances.

1.3 WLAN Controller - Error in mixed installations

(ID 19530)

In WLAN infrastructures managed with the WLAN controller and composed of access points of different types, there were diverse errors ranging from GUI error messages to non-functional access points.

1.4 Hotspot - Memory leak

(ID 19274)

After several days of operating the Hotspot Server, there could be a memory leak.

1.5 WLAN Controller - WTP not managed correctly

(ID 19324)

It could occur that the WLAN Controller managed a slave access point correctly only after the slave had been rebooted.

1.6 Surveillance - Wrong interpretation

(ID 19313)

When a host was monitored by its IP address (***Local Services*** > ***Surveillance***), the host was interpreted as inactive when the value configured for ***Successful Trials*** was larger than the one configured for ***Unsuccessful Trials*** even if the host was actually reachable.

1.7 GUI - Hotspot Timeout

(ID 19290)

It was not possible to deactivate the option Default idle timeout by setting a value of *0* in the menu ***Local Services*** > ***Hotspot Gateway*** > ***New/Edit***.

1.8 Scheduler - Unintended execution

(ID 18745)

Even though the scheduler was deactivated by setting the schedule interval to *0*, it could happen that configured actions were carried out because of different kinds of triggers.

1.9 DynDNS - Authentication failed

(ID 19748)

When using DynDNS, it could happen that authentication failed because the password was cut off.

1.10 SNMP Browser - ipsecPeerTable not changeable

(ID 19222)

In the GUI in the *SNMP Browser* ***VIEW***, it was not possible to change the entries in the MIB table *ipsecPeerTable*.

1.11 WLAN - Multiple stacktraces

(ID 19760)

When using several bridge links, it could happen that at least one bridge link pair did not run stable and caused stacktraces after an uptime of about two days. At the concerned access point, a memory leak occured prior to the stacktrace.

1.12 WLAN - Wrong number of slaves

(ID n/a)

With ***Operation Mode*** = *Bridge Link Client*, more than one slave was activated though this operation mode supports only one slave.

1.13 WLAN Controller - WTP did not work correctly

(ID 19553)

If several WTPs are managed by one WLAN controller, after switching a WTP on and off it could happen that another WTP was in the wrong state.

1.14 Network - Drop in

(ID 19484)

When using a drop-in group, it resulted in two or three reboots per day.

1.15 WLAN Controller - Scan procedure did not start

(ID n/a)

Under specific circumstances, it could happen that a scan procedure initiated by the WLAN controller did not start.

1.16 WLAN - 5 GHz Outdoor operation band not available

(ID 19696)

If under ***WIRELESS LAN*** > ***ADMINISTRATION*** > ***BASIC SETTINGS*** the option ***REGION*** = *France* was selected, ***OPERATION BAND*** = *5 GHz Outdoor* was not available in the ***WIRELESS LAN*** > ***WLAN*** > ***RADIO SETTINGS*** > ***EDIT*** menu.

1.17 WLAN controller - Stacktrace

(ID 19698)

If slave access points were managed by one wireless LAN controller, it could happen that a stackrace occured in a few access points.

1.18 WLAN - Panic

(ID 19678)

At access points in the slave mode, it could happen that a panic occured several times a day.