Read Me
System Software 7.10.6 PATCH 2

Deutsch **Diese Version unserer Systemsoftware ist für die Gateways der Rxxx2- und der RTxxx2-Serie verfügbar.**

Beachten Sie, dass ggf. nicht alle hier beschriebenen Änderungen auf alle oben genannten Geräteserien zutreffen.

Folgende Änderungen sind vorgenommen worden:

1.1 Media Gateway - SIP-Sicherheit verbessert

(ID 15692, n/a)

Bisher konnte ein Ruf aus dem Internet initiiert werden, sofern dem SIP-Client im WAN die Daten eines registrierten Clients aus dem LAN einschließlich des SIP-Passworts bekannt waren.

Der Registrar verhält sich jetzt restriktiver. Standardmäßig ist der Rufaufbau ausschließlich über dieselbe IP-Adresse möglich, unter der die SIP-Registrierung erfolgte. Zudem wird der Zugriff von öffentlichen IP-Adressen ignoriert. Wer den Zugriff wissentlich zulassen möchte, kann das Verhalten in der MIB mit Bit 6 (***HASPUBLICREGIST***) der MIB-Variable ***OPTIONS*** in der MIB-Tabelle ***VOIPSIPEXTENSIONTABLE*** konfigurieren.

Wenn über Port 5060 viele Anfragen (Denial-of-Service-Attacken) gesendet wurden, stieg die CPU-Last bis auf 86 % an und brachte damit die Rufverarbeitung praktisch zum Erliegen.

Zur Abwehr solcher Attacken und zur Begrenzung der Überlast wurden die Grenzwerte erheblich verringert, so dass bei SIP-basierten Attacken Einschränkungen minimiert werden. Wenn die DoS-Attacken von derselben Quell-IP-Adresse stammen, greift die SIP-Session-Begrenzung ein und die CPU-Last wird begrenzt.

1.2 SIP - Eingehende Rufe nicht möglich

(ID 16856)

Die Richtlinien zur Absicherung von SIP-Verbindungen waren so restriktiv ausgefallen, dass eingehende SIP-Invite-Pakete verworfen wurden und keine eingehenden SIP-Rufe möglich waren.

Das Problem ist gelöst.

1.3 GUI - Load Balancing

(ID 16545)

Im Menü ***Netzwerk*** ➜ ***Lastverteilung*** ➜ ***Special Session Handling*** ➜ **Neu** fehlte die Schaltfläche **Erweiterte Einstellungen**.

Das Problem ist gelöst.

1.4 Drop-In-Gruppen funktionierten nicht zusammen mit BootP Relay

(ID 16556)

Wenn eine Drop-In-Gruppe zusammen mit einem DHCP Relay Server konfiguriert war, wurde der DHCP-Datenverkehr auf den Schnittstellen, die zu einer Drop-In-Gruppe gehörten, nicht an den Relay Server weitergeleitet, unabhängig davon, ob als ***Modus*** der Drop-In-Gruppe *Transparent* oder *Proxy* eingestellt war.

Das Problem ist gelöst.

1.5 Proxy ARP funktionierte nicht zusammen mit RADIUS Server

(ID 16253)

Wenn eine IP-Adresse über einen RADIUS Server zugewiesen wurde, wurde Proxy ARP nicht aktiviert. Das Gateway beantwortete daher keine ARP Requests.

Das Problem ist gelöst.

1.6 IPSec - Falscher Wert für MIB-Variable Interface in der MIB-Tabelle ipsecTrafficTable

(ID 16324)

Wenn auf einen RADIUS Preload ein RADIUS Reload folgte, enthielt die MIB-Variable ***INTERFACE*** in der MIB-Tabelle ***IPSECTRAFFICTABLE*** fälschlicherweise den Wert *0*.

Das Problem ist gelöst.

English **This version of our system software is available for gateways of the Rxxx2 and RTxxx2 Series.**

Please note that not all changes listed here necessarily apply to all series of gateways.

The following changes have been made:

1.1 Media Gateway - SIP security improved

(ID 15692, n/a)

Up to now, a call could be initiated from the Internet using the data of a SIP client registered in the LAN including the SIP password.

From now on, the behaviour of the registrar is much more restrictive. By default, setting up a call is only possible with the same IP address that was used for registering. Additionally, any access via public IP address will be ignored. You can allow access from a public IP address in the MIB using Bit 6 (***hasPublicRegist***) of the ***Options*** MIB variable in the ***voipSipExtensionTable*** MIB table.

When many requests (denial of service attacks, DoS attacks) used port 5060, the CPU load rose up to 86 % and call processing nearly broke down.

The restrictions caused by SIP based attacks will be minimized by reducing the threshold values to limit the overload. Receiving too many requests from the same source IP address activates the SIP session limitation and the CPU load does not increase anymore.

1.2 SIP - Incoming calls not possible

(ID 16856)

The policies for securing SIP connections had become so restrictive that incoming SIP invite packets were discarded and no incoming SIP calls were possible.

The problem has been solved.

1.3 GUI - Load Balancing

(ID 16545)

In the ***Networking*** ➜ ***Load Balancing*** ➜ ***Special Session Handling*** ➜ **New** menu the **Advanced Settings** button was missing.

The problem has been solved.

1.4 Drop In Groups failed with BootP Relay

(ID 16556)

When configuring a Drop In Group together with a DHCP Relay Server, the DHCP data traffic of interfaces belonging to a Drop In Group was not forwarded to the Relay Server. Setting ***Mode*** = *Transparent* or ***Mode*** = *Proxy* for the Drop In Group had no effect on this problem.

The problem has been solved.

1.5 Proxy ARP failed with RADIUS Server

(ID 16253)

When an IP address was assigned by a RADIUS Server, Proxy ARP was not activated. Therefore, the gateway did not answer ARP Requests.

The problem has been solved.

1.6 IPSec - Wrong value of the interface variable in the ipsecTrafficTable table

(ID 16324)

When a RADIUS Preload was followed by a RADIUS Reload, the ***INTERFACE*** MIB variable in the ***IPSECTRAFFICTABLE*** MIB table was set wrongly to *0*.

The problem has been solved.

When many requests (denial of service attacks, DoS attacks) used port 5060, the CPU load rose up to 86 % and call processing nearly broke down.

The restrictions caused by SIP based attacks will be minimized by reducing the threshold values to limit the overload. Receiving too many requests from the same source IP address activates the SIP session limitation and the CPU load does not increase anymore.