

Read Me

System Software 7.6.1 PATCH 2

This version of our system software is available for the following gateways:

- **R200 Series**
- **R1200**
- **R3x00 Series**
- **R4x00 Series**
- **Wx002 Series**
- **WI Series**
- **TR200**

Important Security Information

This version of our system software removes the DNS implementation vulnerability VU#800113 described by the US-CERT (see <http://www.kb.cert.org/vuls/id/800113>).

Moreover, the following changes have been made:

1.1 NAT - Number of NAT Ports increased

(ID n/a)

The number of NAT ports has been increased to 32767.

1.2 DNS - Reboot after receiving DNS Requests

(ID n/a)

After receiving a DNS request, the gateway sporadically rebooted.

1

The problem has been solved.

1.3 DNS - Random Source Ports and IDs

(ID n/a)

Since using the same UDP port for all DNS queries and other services has been identified as a severe security risk, random ports and query IDs are used as of now.

1.4 IPSec - No encrypted data traffic

(ID 10526)

When encrypting data traffic in IPSec traffic list mode, no data traffic was possible with a frame size of 4 KByte or larger.

The problem has been solved.

1.5 No Alive Packets sent after connection attempt

(ID n/a)

If an PPP interface with a shorthold of -1 or an IPSEc interface unsuccessfully tried to establish a connection, no Alive Packets were sent after the connection attempt.

The Problem has been solved.

1.6 HTTP - User name and password displayed

(ID n/a)

Username and password of a login were displayed in the browser address bar.

The problem has been solved.

1.7 ATM - Reboot

(ID 10306)

The device rebooted when changing the IP-configuration of an RPoA interface from "DHCP" to "Manual" via the Setup tool.

The Problem has been solved.

1.8 WLAN - Misleading error message

(ID n/a)

If the WLAN channel was set to 12 or 13, and the region was changed to US, the error message "unsupported changes by setup tool" was displayed, since usage of these channels is not permissible in the US.

The problem has been solved.

1.9 QoS - Wrong Tagging

(ID n/a)

QoS tagging on the basis of ipFilter or ipQoSTable entries could be overwritten by subsequently applied SIF rules.

1

The problem has been solved.

1.10 Grep - Malfunction with long strings

(ID n/a)

The grep command did not function if the string entered was longer than 1024 characters.

The problem has been solved.

1.11 Multicast - Memory leak

(ID n/a)

If Multicast protocols were active on the gateway, memory was lost over time.

The problem has been solved.

1.12 Setup Tool - Irrelevant menus shown

(ID 10077)

The Setup Tool displayed the menus for Pre and Post IPSec Rules even in the case of purely interface based configurations. A configuration in these menus could then lead to unexpected results.

The problem has been solved.



Attention!

Generally, it is not recommended to configure any Pre or Post IPSec Rules in a completely interface based IPSec configuration.

In case you have Pre- or Post IPSec Rules defined, these will remain effective after the update. In order to delete them (if necessary) you can create a temporary peer on the basis of traffic lists. The respective menus will then be accessible again, and you can delete any undesired rules. Afterwards you should also delete the temporary peer again.

1.13 Setup Tool - Wrong interface selection PPPoE Passthrough

(ID 10106)

Bridge Group interfaces were not offered for selection when configuring PPPoE Passthrough.

The problem has been solved.

1.14 Setup Tool - WAN Bridge not configurable

(ID n/a)

After the introduction of the new bridge concept, the configuration of a WAN Bridge was not possible using the Setup Tool.

The problem has been solved.

1.15 INET - TFTP/L2TP connection failure

(ID n/a)

If a previous TFTP or L2TP connection had not timed out, further connections using the same source port failed.

The problem has been solved.

1.16 QoS - TDR entry not saved correctly

(ID n/a)

If an existing TDR entry was duplicated, the duplicate entry was silently deleted, but so was the original one. It was necessary to save the entry twice to successfully write it to the configuration.

The problem has been solved.

1.17 TDR - Data traffic blocked

(ID n/a)

If TDR was activated for an already active connection, all TCP traffic was occasionally blocked until the connection was closed and reestablished.

The problem has been solved.