Readme for System Software 7.2.2 PATCH 2

The following changes have been made to System Software 7.2.2 in order to improve performance and stability. Make sure to check the Release Notes of the major release corresponding to this PATCH release for specifics concerning update procedures and restrictions.

Important: IPSec Vulnerability Fixed

Funkwerk gateways were affected by an ISKAMP vulnerability that was detected at http://www.ee.oulu.fi (see http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/). They failed the following test cases: #16, #427, #1681 and #2970.

Susceptibility to the vulnerability has been removed.

1) SIF Prevents TFTP Transfer

With SIF activated, the necessary sessions were not created to allow actual data transfer.

This problem has been solved.

2) Decimal Notation for OIDs (ID n/a)

By using the `x` command on the SNMP shell, it is possible to enter OIDs in a decimal notation. This led to errors in the identification of the intended MIB.

This problem has been solved.

3) NAT Debug Messages Suppressed (ID 4268)

Debug messages from the NAT system were not displayed when using the `debug` command on a level that would usually show this kind of information (e.g. `debug all`).

This problem has been solved.

4) Post IPSec Traffic - Remote Type not Configurable (ID 3934)

The type for the remote side of Post IPSec Traffic configuration in [IPSec > Post IPSec Rules > EDIT/APPEND] was not configurable.

This problem has been solved.

5) Stack Trace with IP Load Balancing (ID 4301)

Using IP Load Balancing for GRE sessions that were not used by PPTP connections led to a stack trace.

This problem has been solved.

6) Stack Trace with Syslogs (ID n/a)

A stack trace was occasionally created when Syslog tried to access certain traps.

This problem has been solved.

7) Certificate Server Cannot be Deleted (ID 4428)

Once an entry had been created in the certServerTable (either via the Setup Tool or on the SNMP shell), the configuration could no longer be deleted.

This problem has been solved.

8) NAT Session Restriction not Applied Correctly

Restricting the maximum number of NAT sessions (by setting ipExtIfNatMaxSessions) did not work exactly as expected: One additional session was allowed.

This problem has been solved.

9) "Decode failed" Error Message (ID 4235)

Under certain conditions, all UDP packets coming from the network(s) connected to the gateway were treated as SNMP responses causing the gateway to display an error on accessing the MIB.

This problem has been solved.

10) Certificate / CRL Download Failed (ID 4598)

An automatic download of a certificate or a CRL from a server from the certServerTable failed because the request was sent to a wrong port.

This problem has been solved.

11) Impossible to Add Post IPSec Rule (ID 4586)

Once a first Post IPSec Rule had been configured, the gateway crashed when trying to add a further one.

This problem has been solved.

12) Panic with Error in IPSec (ID 4708)

Occasionally, the gateway reboots, displaying an IPSec related error message on the serial console.

This problem has been solved.

13) Authentication Failure (ID 4771)

When authentication was carried out in a multi-step process, occasional failures occurred.

This problem has been solved.

14) MIB Search Operations Failed (ID 4767)

Search operations inside the MIB could fail.

This problem has been solved.

15) MIB Tables Missing in Administration Group (ID 4775)

The tables biboAdmLoginTable and biboAdmLicenseTable were missing in the Administration group of MIB tables.

This problem has been solved.

16) New Start Mode for IPSec Peers

To ensure an IPSec tunnel is created immediately after the gateway is booted, a new parameter has been introduced for peer configuration. [IPSec > Configure Peers > APPEND/EDIT > Peer specific Settings] now offers the choice between `Start Mode Always Up` and `On Demand`. If set to `Always Up` , the gateway will try to create a tunnel as soon as the gateway has been booted.