Service Release Notes for WiNG 5.9.1.3-007R

Please Note: Service releases are made available to fix specific customer reported issues in a timely manner. Service releases are not as extensively tested as main releases (such as 5.9.1.0-029R). The next maintenance or manufacturing release will incorporate all qualifying and preceding service releases.

This document is an addendum to the release notes for the main release 5.9.1.0-029R.

Contents

- Resolved Issues
- Platforms supported
- Upgrade/Downgrade Process

Resolved Issues

This service release 5.9.1.3-007R contains important fixes for customer reported issues and several enhancements.

Additional Enhancements:

Korea regulatory – AP 8533 certified to operate in Korea.

Following vulnerabilities addressed in this release:
CVE-2018-5787 – Remote unauthenticated stack overflow in RIM module thru UDP port 3799.
CVE-2018-5788 – Remote and unauthenticated denial of service attack in RIM module thru UDP port 3799.
CVE-2018-5791, CVE-2018-5792, CVE-2018-5793 – Remote and unauthenticated heap overflow in HSD process over MINT Protocol.
CVE-2018-5790 – Remote unauthenticated global denial of service in RIM over MINT Protocol.
CVE-2018-5789 – Remote and unauthenticated XML entity expansion vulnerability can cause denial of service.
CVE-2018-5795 – Arbitrary file write from WebGUI by low access user.
CVE-2018-5796 – By reverse engineering root access password generator – it might be possible to access root shell for WiNG OS.

Following is a list of SPRs/CRs fixed in this release:

SPR/CQ	Description
SPR-3398	When ExtremeLocation server is configured but not available, AP will go out of memory
SPR-3402	NX 5500E - GUI Login Opens to A Blank Page due to missing Google client ID
SPR-3403	EGuest: New factory default AP does not get template pages from controller on adoption
SPR-3405	AP 7532 not able to send data - NAR queue is full
SPR-3407	DPD2 crash during L2TPv3 tunnel activation time upon failover
SPR-3415	GUI error when enabling auto upgrade for AP 76XX series

SPR/CQ	Description
SPR-3418	LSP DB contains entries with sequence number and adjacency 0 leading to corruption
WING-34869	EGuest: Usage data shows abnormal data in two days, where the total amount of traffic upstream was less than 500GB
WING-35406	Kernel panic and treegen core on AP 6521 while attaching ACL
WING-36134	Not all filters are saved in AVC client count trend widget
WING-36164	EGuest: Support added for providing sender phone no. (Long/short code) in notification policy
WiNG-36165	EGuest licensing - only count Aps that use EGuest as part of the license
WING-36194	NSight: AVC: "All application by usage" widget does not display any client
WING-36214	NSight: AVC: Mismatch in query and output displayed for App Group Trend widget
WING-36216	Data rate shows as 1MB on AP 76XX radios on all packets on both radios on packet capture
WING-36217	cfgd crash due to communication break between cfgd and dpd2 - KeyError: 'domain_name'
WING-36308	EGuest help link was broken in the previous releases

Important notes:

- Occasionally a mismatch is seen between the left navigation tree selection and actual data displayed on dashboard widget. User needs to refresh the dashboard using the refresh button on the top right corner.
- Only below mentioned filter options are supported for Application Group/Application and AVC Client count trend widgets.
  Application Group Widget –
    o User can view all applications usage across all WLANs.
    o User can view a specific application usage across all WLANs.
    o User can view a specific application usage for a specific WLAN.
    o Application Group is not supported in the Application Group/Application Filter.

  Application Group Trend Widget -
    o User can view the Application usage trend for specific application across all WLANs.
    o User can view the Application usage trend for specific application grp across all WLANs.
    o WLAN Filter for a specific WLAN is not supported. Irrespective of the selected WLAN, trend will be displayed for all WLANs.

- For Guest clients (WLAN marked with "no nsight client-history"), "All Applications By Usage" Widget will display only the count and Tx/Rx of the applications. Details of clients accessing the applications will not be shown in this release.

2. Platforms Supported

This release applies to all platforms released with WiNG 5.9.1.0-029R.

Reminder:
Dependent AP platforms: AP 621, 622, 650 are EOL and engineering support has ended.

Independent AP platforms: AP 6511, AP 6511E, AP 7131, AP 7181, AP 8222, ES 6510 are EOL and engineering support has ended.
Controller platforms: RFS 4011, RFS 7000, NX 9000, NX 45XX and NX 65XX platforms are EOL and engineering has ended.

3. Firmware Upgrade/Downgrade Procedure

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

For detailed upgrade procedure – please refer to WiNG 5.9.1 release notes.

Upgrade from WiNG v5.x.x.x to WiNG v5.9.1.x

1. Copy the controller image to your tftp/ftp server.

2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>‖**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is —reload.