Service Release Notes for WiNG 5.8.6.9-003R

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 5.8.6.0-011R). 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 5.8.6.0-011R.

Contents

Resolved Issues

This service release 5.8.6.9-003R contains important vulnerability fixes as well as fixes for customer reported issues.

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 changes in this release:

SPR/CQ	Description
WING-35406	Kernel panic and treegen core on AP 6521 while attaching ACL
WING-36195	Panic seen on AP 7532 at “PC is at free_packet”
WING-36409	Random dpd2 crashes seen when hash table has stale entries
SPR-3405	AP 7532 not able to send data - NAR queue is full
SPR-3407	DPD2 crash during L2TPv3 tunnel activation time upon failover

2. Platforms Supported

This release applies to all platforms released with WiNG 5.8.6.0-011R.

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 5.8.6 release notes.

Upgrade from WiNG v5.x.x.x to WiNG v5.8.6.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.