# Maintenance Release Notes

WiNG 5.9.1.11-002R

## Contents



## Features

### Frag Attack Fix

This release addresses the frag attacks vulnerability issues in the 802.11 standard and implementations **only for AP75XX Broadcom platforms.**

Please see the Vulnerability section for details of CVE fixed in this release.

## Commands

None.

# Updates

# Fixed Issues

Following issues are fixed.

| ESR/SPR | Description |
|---|---|
| WOS-2750 | Broadcom patches for FragAttacks vulnerabilities |
| WING-44010 | WiNG 5.9.1.10 trap sent for Device offline missing RF-domain |

# Known Issues

- None.

# Vulnerabilities Updates

**CVE-2020-24588: Accepting non-SPP A-MSDU frames**: The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SPP A-MSDU frames, which is mandatory as part of 802.11n, an adversary can abuse this to inject arbitrary network packets

**CVE-2020-24587: Reassembling fragments encrypted under different keys:** The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed

**CVE-2020-24586: Not clearing fragments from memory when (re)connecting to a network:** The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments must be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data

# Firmware Upgrade/Downgrade

## Preparations

- Create backup of current configuration before starting procedure.
- Ensure proper and uninterrupted power supply to devices during the procedure.
- Both controller and AP should be upgraded or downgraded to same version.
- Upgrade should be done on controller(s) first followed by AP(s).

- Downgrade should be done on AP(s) first followed by controller(s).

### Manual Install (CLI/GUI)

- Download appropriate device image(s) to TFTP/FTP/SFTP server.
- From CLI, use either of following commands,
  - `upgrade ftp://<username>:<password>@<server>/<name of file>`
  - `upgrade sftp://<username>:<password>@<server>/<name of file>`
  - `upgrade tftp://<server>/<name of file>`
- From GUI,
  - `Switch→Firmware→Update Firmware`
- Reload device via CLI command or from GUI

### Auto Install (DHCP)

This mechanism works via the DHCP protocol by defining Vendor Class and three other sub-option that can be either sent separately or under Option 43. The three options are,

- Option 186 – String in `<ftp|sftp|tftp>//<username>:<password>@<server>` format
- Option 187 – String defining firmware path and filename
- Option 188 – String defining configuration path and filename

Make sure `ip dhcp client request options all` is configured in interface configuration.

Following are DHCP Vendor Class identifiers for WiNG devices,

- WingRFS.RFS4010
- WingNX.NX9500
- WingAP.AP8163
- WingAP.AP7532
- WingAP.AP7612
- WingAP.AP8432
- WingNX.NX5500
- WingNX.NX9600
- WingAP.AP7502
- WingAP.AP7562
- WingAP.AP7622
- WingAP.AP8533
- WiNGNX.NX7500
- WiNGVX.VX9000

WingAP.AP7522
WingAP.AP7602
WingAP.AP7632

# Controller Platform Install Notes

# AP Platform Install Notes

### AP7522/AP7532/AP7562

- AP7522, AP7532, and AP7562 manufactured after July 2017 use new NAND chip. Downgrading to a release prior to WiNG 5.8.0 will render these units irrecoverable. Please refer field flash "FN-417 – AP 7522, AP 7532, AP 7562 Component Change" for the affected hardware revision and software downgrade version restrictions.
- When downgrading from WiNG 5.8 to WiNG 5.5.5 or WiNG 5.5.4 on AP7532/7522, the user needs to apply kernel patch `AP75XX-CPU-Bringup-1.0.patch`. AP7532/AP7522 running WiNG 5.5.6/5.7.x has an updated kernel version and the patch is required when the AP downgrades to a firmware with a prior kernel version. Use following steps to apply patch,
  - Copy `AP75XX-CPU-Bringup-1.0.patch` to your ftp/sftp/tftp server.
  - Apply the patch using upgrade command.

- Use “boot system primary” or “boot system secondary" based on the WiNG 5.5.5/5.5.4 image location on the AP.
- Reload.

# Platforms Support

Supported in this release,

AP7522, AP7532, AP7562

# Notes