Maintenance Release Notes

WiNG 5.9.8.0-002R

Contents

Features

WiNG-XIQ Secure Communication

Abhijit Chandavale, Dominic Velikakath Peter

This release introduces secure mechanism for WiNG devices to post configuration and periodic statistics to XIQ. The secure and encrypted channel is established by validating server certificate of XIQ by WiNG controllers and access points followed by device level unique username/password-based authentication by XIQ.

Any WiNG firmware version prior to this feature will continue to establish unsecure communication with XIQ and should be used only in non-production environments.

At any time, WiNG can only be configured with either NSight server hostname or IP address or XIQ URL.

Commands

1. Configuring XIQ URL

   WiNG uses existing NSight policy server command for XIQ communication. The same command can be set to XIQ URL va-gcp-wing.extremecloudiq.com.

```
vx9000-8D09E7(config)#nsight-policy CLIENT
vx9000-8D09E7(config-nsight-policy-CLIENT)#show context
nsight-policy CLIENT
 server host 10.234.165.41 https

vx9000-8D09E7(config-nsight-policy-CLIENT)#no server host 10.234.165.41
vx9000-8D09E7(config-nsight-policy-CLIENT)#commit
vx9000-8D09E7(config-nsight-policy-CLIENT)#server host va-gcp-
wing.extremecloudiq.com https enforce-verification
vx9000-8D09E7(config-nsight-policy-CLIENT)#commit write memory
vx9000-8D09E7(config-nsight-policy-CLIENT)#
```

2. Installing/updating XIQ CA certificate. This command is optional as XIQ CA certificates will be included in the release. This command is useful when XIQ CA certificate needs to be changed.

   This is a new command to install/update XIQ CA certificate on WiNG devices.

```
CORP-WING1# copy xiq-cachain from ?
  URL  Location of CA certificate
       URLs:  tftp://<hostname|IP>[:port]/path/file
              ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
              sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file
              http://<hostname|IP>[:port]/path/file
              cf:/path/file
              usb<n>:/path/file
       IPv6 URLs:   tftp://<hostname|[IPv6]>[:port]/path/file
              ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file
              sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]>/path/file
              http://<hostname|[IPv6]>[:port]/path/file
```

3. Enforcing security and encryption

   The existing configuration command for specifying NSight Server (or XIQ) URL will have additional optional parameter **enforce-verification** in order to trigger certificate validation process.

   - If parameter is not configured, then WiNG device shall try to establish connection with a NSight server using existing mechanism.
   - If parameter is configured, then WiNG device shall try to establish connection with XIQ by validating XIQ certificate and username/password-based authentication.

```
vx9000-8D09E7#show run nsight-policy CLIENT
nsight-policy CLIENT
 server host va-gcp-wing.extremecloudiq.com https enforce-verification
vx9000-8D09E7#
```

Updates

- Fixes an issue in configuration playback during upgrade and downgrade procedure when APs and controllers are at different versions.
- Fixes WING.MIB to return system memory in MBs instead of KBs.
- Adds UI support for configuring wired 802.1x EAP-TLS configuration.
- Fixes AP high CPU utilization on AP76XX platforms when running in sensor mode.
- Fixes AP panics caused by malformed/crafted DNS packet handing when captive-portal is configured.
- Add recovery and resiliency to recovery of startup-configuration in event of a filesystem corruption.

Fixed Issues

Following customer issues are fixed.

ESR/SPR	Description
WING-42413	AP7632 5.9.6 many different crashes
WING-42639	Kr00k Vulnerability CVE-2019-15126
WING-42563	When controller host is configured as hostname via CLI and DHCP option 191. Adopted AP continue to send Mint Mlcp packets every 1 minute.
WING-42287	CDP LLDP element missing under WiNG adoption info
WING-38907	SPR-3633: AP7602 interface ge2 auto negotiation failed with same platform
WING-42203	Multiple ping lost observed
WING-42733	WING-MIB.mib description indicate Total system ram in megabytes. but return value is kilobytes
WING-42499	AP can't update its startup-config because of checksum issue
WING-42381	AP7662 Core crash
WING-42828	Channel and RSSI always 0
WING-39253	SPR-3662: Onboard WIPS Rogue/Unsanctioned Events UI displays SSID, Syslog does not display SSID
WING-42111	In GUI a Read-only account exposes the snmp v1/v2 read/write community string

Known Issues

- Possible AP panic on AP7522/AP7532/AP7562/AP8432/AP8533 when radios are disabled prior to upgrade and re-enabled post reload. Workaround is not to disable/change radio configuration prior to upgrade.

Vulnerabilities Updates

Patches are applied to existing versions of components to address reported vulnerabilities. However, some tools only check for versions against reported CVEs instead of checking for fixes. Such tools will continue to report vulnerabilities.

1. **CVE-2019-15126**
   Kr00k is a vulnerability that permits attackers to force Wi-Fi systems into dissociative states, granting the opportunity to decrypt packets sent over WPA2 Personal/Enterprise Wi-Fi channels. This vulnerability is specific to Broadcom based APs. When handling a disassociation event for a peer (both AP and STA), keys are deleted first. When the keys are deleted from software, the all-0s key is written to HW. Further packets from the stack are not accepted or queued to the hardware for transmit. Traffic that has already been queued to the hardware for the peer is not flushed immediately. During the time window in disassociation processing, where after a key is deleted, frames already buffered in HW FIFOs are transmitted with the all-0s key. Such dissociation may be induced by ioctl/iovar commands from host software, a disassociate/deauthentication message from the peer, or over the air from an attacker. The exposed security vulnerability is that the frames sent from the AP with the all-0s key can be decrypted without knowledge of the original security keys.

DFS Support

Model	**Master DFS**				**Client DFS**			
	FCC	IC	ETSI	Japan	FCC	IC	ETSI	Japan
AP8163		•	•			•	•	
AP7502	•	•	•	•				
AP7522	•	•	•	•	•	•	•	•
AP7532	•	•	•	•	•	•	•	•
AP7562	•	•	•	•	•	•	•	•
AP7602	•	•	•		•	•		
AP7622	•	•	•	•	•	•	•	•
AP7612	•	•	•		•		•	
AP7632	•	•	•		•		•	
AP7662	•		•	•	•		•	•
AP8432	•		•	•	•		•	•
AP8533	•		•	•	•		•	•

AirDefence Sensor Capabilities Support

Dedicated Radio(s)

AirDefence sensor capability matrix as supported on 802.11n/ac APs for WIPS and network assurance functionalities when radio(s) are in dedicated mode.

Model	WIPS & Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Test	Connection Troubleshooting	Wireless Vulnerability Assessment
AP8163	•		•	•	•	•	•	•
AP7502								
AP7522[1]	•		•	•	•	•	•	•
AP7532[1]	•		•	•	•	•	•	•
AP7562[1]	•		•	•	•	•	•	•
AP7602	•				•			
AP7612[1]	•		•		•			
AP7622	•				•			
AP7632[1]	•		•		•			
AP7662[1]	•		•		•			
AP8432[2]	•		•	•	•	•	•	•
AP8533[3]	•		•		•	•	•	•

[1] Radios are band-locked so entire AP will act as a dedicated sensor.
[2] Only radio 1 is available as a dedicated sensor.
[3] Only radio 3 is available as a dedicated sensor.

Radio-Share

AirDefence sensor capability matrix as supported on 802.11n/ac APs for WIPS and network assurance functionalities when radio(s) are in radio-share mode.

Model	WIPS & Advanced Forensics	Spectrum Analysis[1]	Advanced Spectrum Analysis[2]	Live RF	Live View	AP Test[3]	Connection Troubleshooting	Wireless Vulnerability Assessment
AP8163			•	•	•	•	•	
AP7502								
AP7522[4]	•			•	•		•	
AP7532[4]	•			•	•		•	
AP7562[4]	•			•	•		•	
AP7602								
AP7612[4]	•				•			
AP7622								
AP7632[4]	•				•			
AP7662[4]	•				•			
AP8432	•				•		•	
AP8533								

[1] Spectrum analysis is not supported in radio-share mode.
[2] Advanced spectrum analysis impacts WLAN performance in radio-share mode.
[3] Only single cell/internal BSS testing is supported.
[4] Both radios are band locked and both radios MUST be in radio-share mode for sensing.

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

When upgrading from prior versions, new profiles for newly supported platforms will not be present in the startup-config. The user can either create a default profile or do `erase startup-config`.

VX9000

Secondary Storage

VX9000 has a limitation of default disk size of 2TB. This is addressed by adding a secondary storage.

- Enabling secondary storage does not copy data files to the new location.
- It is recommended immediately after provisioning the guest instance, before enabling NSight or Captive Portal.

- If the secondary storage needs to be enabled after NSight/Captive Portal, it is recommended to back up the database, and restore the database after secondary storage is enabled.
- If the VX9000 instance is not a primary (replica-set member), the database server will perform full data sync after it is restarted with the new secondary storage.

NSight/Captive Portal

VX9000 requires re-install using the VX9000-INSTALL-5.8.2.0-030R.ISO image if the user intends to configure NSight/Captive Portal functionality. This is due to the changes to the flash partition (25% of the allocated disk size – 4GB Min, 128GB Max) to take effect.

- Export configuration before reinstalling the VX.
- To preserve the same MAC address (and therefore the serial number for licensing)
    - Delete current hard disk from the VM
    - Add new virtual hard disk
    - Connect ISO file as virtual CD
    - Boot into CD to start installation process
- After installation is complete, restore the configuration.

NX9600

- WiNG 5.8.6 introduced support for new RAID controller for NX 9600 platform. For platforms shipping with new RAID – downgrade below v5.8.6 will be disallowed.
- WiNG 5.8.1 changed default RAID configuration for NX 9600 from RAID 5 to RAID 10 to improve performance. RAID configuration cannot be changed upon upgrade or downgrade.
- NX 9600 controllers manufactured with v5.8.1 or above will have RAID 10 configured. NX 9600 controllers manufactured with v5.5.6 will have RAID 5 configured.
- RAID configuration can only be changed by authorized personnel.

RFS4000

When downgrading an RFS4000 from WiNG 5.8 to WiNG 5.7, the user first needs to downgrade the RFS4000 to WiNG 5.7.2 before moving to WiNG 5.7.

AP Platform Install Notes

AP8533/AP8432

- AP 8533/8432 manufactured with v5.8.4 or above cannot be downgraded to v5.8.3.
- When upgrading AP 8533 running v5.8.3.x to v5.8.6, please upgrade to v5.8.4 first and then to v5.8.6.

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.

AP81XX

- WiNG 5.8.1 added support for new NAND chipset for AP8122, AP8132, AP8163, AP8222 and AP8232. APs manufactured with new NAND cannot be downgraded to the prior version.
- WiNG 5.5.2 added support for new NAND for AP 8XXX platforms. Downgrade to prior releases on hardware with new NAND will be blocked.

Platforms Support

Supported in this release,

AP8163, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000

Notes

This WiNG release is compatible with XIQ release Q1R2 version 20.2.0.3 and above.