# AOS-S Switch 16.11.0015 Release Notes

aruba

a Hewlett Packard
Enterprise company

# Contents

These release notes include the following topics:

- Important Information
- Terminology Change
- Version History
- Security Bulletin Subscription Service
- Compatibility/Interoperability
- Platforms and Minimum Supported Software Versions

## Important Information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

## Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

| Usage | Old Language | New Language |
|---|---|---|
| Switch Security | Master | Main |
| Switch Routing | Master | Main Router |
| Smart Link | Master-Slave | Primary-Secondary |
| Chassis Events, IPv6 Configuration, and Troubleshooting | Master-Slave | Management-Slot |
| Switch Stack | Master-Slave | Conductor-Member |
| Switch Security, Configuration and Routing | Blacklist, Whitelist | Denylist, Allowlist |
| Route Type | Blackhole Route | Null Route |
| Type of Hackers | Black Hat, White Hat | Unethical, Ethical |

# Version History

NOTE

All released versions are fully supported by Hewlett Packard Enterprise, unless noted in the table.

**Table 1:** *Version History*

| Version number | Software | Release Date | Remarks |
|---|---|---|---|
| 16.11.0015 | KB, WC, YC, and YA/YB | 2023-11-27 | Released, fully supported, and posted on the web. |
| 16.11.0014 | KB, WC, YC, and YA/YB | 2023-09-22 | Released, fully supported, and posted on the web. |
| 16.11.0013 | KB, WC, YC, and YA/YB | 2023-07-31 | Released, fully supported, and posted on the web. |
| 16.11.0012 | KB, WC, YC, and YA/YB | 2023-05-29 | Released, fully supported, and posted on the web. |
| 16.11.0011 | KB, WC, YC, and YA/YB | 2023-04-10 | Released, fully supported, and posted on the web. |
| 16.11.0010 | KB, WC, YC, and YA/YB | 2023-02-15 | Released, fully supported, and posted on the web. |
| 16.11.0009 | KB, WC, YC, and YA/YB | - | Version 16.11.0009 is unavailable for download. |
| 16.11.0008 | KB, WC, YC, and YA/YB | 2022-11-14 | Released, fully supported, and posted on the web. |
| 16.11.0007 | KB, WC, YC, and YA/YB | 2022-10-03 | Released, fully supported, and posted on the web. |
| 16.11.0006 | KB, WC, YC, and YA/YB | 2022-07-29 | Released, fully supported, and posted on the web. |
| 16.11.0005 | KB, WC, YC, and YA/YB | 2022-05-30 | Released, fully supported, and posted on the web. |
| 16.11.0004 | KB, WC, YC, and YA/YB | 2022-03-16 | Released, fully supported, and posted on the web. |
| 16.11.0003 | KB, WC, YC, and YA/YB | 2021-12-13 | Released, fully supported, and posted on the web. |
| 16.11.0002 | KB, WC, YC, and YA/YB | 2021-09-30 | Released, fully supported, and posted on the web. |
| 16.11.0001 | KB, WC, YC, and YA/YB | 2021-09-13 | Initial release of the 16.11 branch. Released, fully supported, and posted on the web. |

# Security Bulletin Subscription Service

You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_ sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via

email.

## Compatibility/Interoperability

The switch web agent supports the following web browsers:

- Internet Explorer- Edge, 11
- Chrome- 53, 52
- Firefox- 49, 48
- Safari (MacOS only)- 10, 9

> **NOTE**
>
> HPE recommends using the most recent version of each browser as of the date of this release note.

## Platforms and Minimum Supported Software Versions

This release is applicable to the following platforms and their respective switches:

- [KB 16.11](#)
- [WC 16.11](#)
- [YA/YB 16.11](#)
- [YC 16.11](#)

### KB 16.11

This release applies to the following Aruba 5400R Switch Series and Aruba 3810M Switch Series:

**Table 2:** *Products Supported*

| Product number | Description |
|---|---|
| J9821A | Aruba 5406R zl2 Switch |
| J9823A | Aruba 5406R 44G PoE+/2SFP+ (No PSU) v2 zl2 Switch |
| J9824A | Aruba 5406R 44G PoE+/4SFP (No PSU) v2 zl2 Switch |
| J9822A | Aruba 5412R zl2 Switch |
| J9825A | Aruba 5412R 92G PoE+/2SFP+ (No PSU) v2 zl2 Switch |
| J9826A | Aruba 5412R 92G PoE+/4SFP (No PSU) v2 zl2 Switch |
| J9868A | Aruba 5406R 8XGT/8SFP+ (No PSU) v2 zl2 Switch |
| JL001A | Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch |
| JL002A | Aruba 5406R 8 port 1/2.5/5/10GBASE T PoE+ / 8 port SFP+ (No PSU) v3 zl2 Switch |
| JL095A | Aruba 5406R 16 port SFP+ (No PSU) v3 zl2 Switch |
| JL003A | Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch |

| Product number | Description |
|---|---|
| JL071A | Aruba 3810M 24G 1 slot Switch |
| JL072A | Aruba 3810M 48G 1 slot Switch |
| JL073A | Aruba 3810M 24G PoE+ 1 slot Switch |
| JL074A | Aruba 3810M 48G PoE+ 1 slot Switch |
| JL075A | Aruba 3810M 16SFP+ 2 slot Switch |
| JL076A | Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1 slot Switch |

## Minimum Supported Software Versions

NOTE

If your switch or module is not listed in the below table, it runs on all versions of the software.

**Table 3:** *Minimum Supported Software Versions*

| Product number | Product name | Minimum software version |
|---|---|---|
| J9986A | HPE 24-port 10/100/1000BASE-T PoE+ MACsec v3 zl2 Module | KB.15.17.0003 |
| J9987A | HPE 24-port 10/100/1000BASE-T MACsec v3 zl2 Module | KB.15.17.0003 |
| J9988A | HPE 24-port 1GbE SFP MACsec v3 zl2 Module | KB.15.17.0003 |
| J9989A | HPE 12-port 10/100/1000BASE-T PoE+ / 12-port 1GbE SFP MACsec v3 zl2 Module | KB.15.17.0003 |
| J9990A | HPE 20-port 10/100/1000BASE-T PoE+ / 4-port 1G/10GbE SFP+ MACsec v3 zl2 Module | KB.15.17.0003 |
| J9991A | HPE 20-port 10/100/1000BASE-T PoE+ / 4p 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module | KB.15.17.0003 |
| J9992A | HPE 20-port 10/100/1000BASE-T PoE+ MACsec / 1-port 40GbE QSFP+ v3 zl2 Module | KB.15.17.0003 |
| J9993A | HPE 8-port 1G/10GbE SFP+ MACsec v3 zl2 Module | KB.15.17.0003 |
| J9995A | HPE 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 zl2 Module | KB.15.17.0003 |
| J9996A | HPE 2-port 40GbE QSFP+ v3 zl2 Module | KB.15.17.0003 |
| JH231A | HPE X142 40G QSFP+ MPO SR4 Transceiver | KB.15.17.0003 |
| JH232A | HPE X142 40G QSFP+ LC LR4 SM Transceiver | KB.15.17.0003 |
| JH233A | HPE X142 40G QSFP+ MPO eSR4 300M XCVR | KB.15.17.0003 |

| Product number | Product name | Minimum software version |
|---|---|---|
| JH234A | HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable | KB.15.17.0003 |
| JH235A | HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable | KB.15.17.0003 |
| JH236A | HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable | KB.15.17.0003 |
| JL001A | Aruba 5412R 92GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch | KB.15.17.0003 |
| JL002A | Aruba 5406R 8-port 1/2.5/5/10GBASE-T PoE+ / 8-port SFP+ (No PSU) v3 zl2 Switch | KB.15.17.0003 |
| JL003A | Aruba 5406R 44GT PoE+ / 4SFP+ (No PSU) v3 zl2 Switch | KB.15.17.0003 |
| JL095A | Aruba 5406R 16-port SFP+ (No PSU) v3 zl2 Switch | KB.15.17.0003 |
| JL075A | Aruba 3810M 16SFP+ 2-slot Switch | KB.16.01.0004 |
| JL071A | Aruba 3810M 24G 1-slot Switch | KB.16.01.0004 |
| JL073A | Aruba 3810M 24G PoE+ 1-slot Switch | KB.16.01.0004 |
| JL076A | Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch | KB.16.01.0004 |
| JL072A | Aruba 3810M 48G 1-slot Switch | KB.16.01.0004 |
| JL074A | Aruba 3810M 48G PoE+ 1-slot Switch | KB.16.01.0004 |
| JL081A | Aruba 3810M/2930M 4 1/2.5/5/10 GbE HPE Smart Rate Module | KB.16.04.0008 |
| JL308A | Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver | KB.16.04.0008 |
| JL745A | Aruba 1G SFP LC SX 500m MMF TAA XCVR | KB.16.10.0007 |
| JL746A | Aruba 1G SFP LC LX 10km SMF TAA XCVR | KB.16.10.0007 |
| JL747A | Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR | KB.16.10.0007 |
| JL748A | Aruba 10G SFP+ LC SR 300m MMF TAA XCVR | KB.16.10.0007 |
| JL749A | Aruba 10G SFP+ LC LR 10km SMF TAA XCVR | KB.16.10.0007 |

**NOTE**

For information on networking application compatibility, see the Software Feature Support Matrix.

## WC 16.11

This release applies to the following Aruba 2930F Switch Series and Aruba 2930M Switch Series:

**Table 4:** *Products Supported*

| Product number | Description |
|---|---|
| JL253A | Aruba 2930F 24G 4SFP+ Switch |
| JL254A | Aruba 2930F 48G 4SFP+ Switch |
| JL255A | Aruba 2930F 24G PoE+ 4SFP+ Switch |
| JL256A | Aruba 2930F 48G PoE+ 4SFP+ Switch |
| JL258A | Aruba 2930F 8G PoE+ 2SFP+ Switch |
| JL259A | Aruba 2930F 24G 4SFP Switch |
| JL260A | Aruba 2930F 48G 4SFP Switch |
| JL261A | Aruba 2930F 24G PoE+ 4SFP Switch |
| JL262A | Aruba 2930F 48G PoE+ 4SFP Switch |
| JL263A | Aruba 2930F 24G PoE+ 4SFP+ TAA-compliant Switch |
| JL264A | Aruba 2930F 48G PoE+ 4SFP+ TAA-compliant Switch |
| JL319A | Aruba 2930M 24G 1-slot Switch |
| JL320A | Aruba 2930M 24G PoE+ 1-slot Switch |
| JL321A | Aruba 2930M 48G 1-slot Switch |
| JL322A | Aruba 2930M 48G PoE+ 1-slot Switch |
| JL323A | Aruba 2930M 40G 8SR PoE+ 1-slot Switch |
| JL324A | Aruba 2930M 24SR PoE+ 1-slot Switch |
| JL557A | Aruba 2930F 48G PoE+ 4SFP 740W Switch |
| JL558A | Aruba 2930F 48G PoE+ 4SFP+ 740W Switch |
| JL559A | Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch |
| JL692A | Aruba 2930F 8G PoE+ 2SFP+ TAA Switch |
| JL693A | Aruba 2930F 12G PoE+ 2G/2SFP+ Switch |
| R0M67A | Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch |
| R0M68A | Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch |

## Minimum Supported Software Versions

If your switch or module is not listed in the below table, it runs on all versions of the software.

**Table 5:** *Minimum Supported Software Versions*

| Product number | Product name | Minimum software version |
|---|---|---|
| JL078A | Aruba 3810M/2930M 1-port QSFP+ 40GbE Module | WC.16.04.0004 |
| JL083A | Aruba 3810M/2930M 4-port 100M/1G/10G SFP+ MACsec Module | WC.16.04.0004 |
| JL308A | Aruba 40G QSFP+ LC Bidirectional 150m MMF 2-strand Transceiver | WC.16.04.0008 |
| JL323A | Aruba 2930M 40G 8SR PoE+ 1-slot Switch | WC.16.04.0008 |
| JL324A | Aruba 2930M 24SR PoE+ 1-slot Switch | WC.16.04.0008 |
| JL557A | Aruba 2930F 48G PoE+ 4SFP 740W Switch | WC.16.05.0003 |
| JL558A | Aruba 2930F 48G PoE+ 4SFP+ 740W Switch | WC.16.05.0003 |
| JL559A | Aruba 2930F 48G PoE+ 4SFP+ 740W TAA-compliant Switch | WC.16.05.0003 |
| R0M67A | Aruba 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch | WC.16.07.0002 |
| R0M68A | Aruba 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch | WC.16.07.0002 |
| J9142B | HPE X122 1G SFP LC BX-D Transceiver | WC.16.07.0003 |
| J9143B | HPE X122 1G SFP LC BX-U Transceiver | WC.16.07.0003 |
| JL692A | Aruba 2930F 8G PoE+ 2SFP+ TAA Switch | WC.16.08.0005 |
| JL693A | Aruba 2930F 12G PoE+ 2G/2SFP+ Switch | WC.16.10.0001 |
| JL745A | Aruba 1G SFP LC SX 500m MMF TAA XCVR | WC.16.10.0007 |
| JL746A | Aruba 1G SFP LC LX 10km SMF TAA XCVR | WC.16.10.0007 |
| JL747A | Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR | WC.16.10.0007 |
| JL748A | Aruba 10G SFP+ LC SR 300m MMF TAA XCVR | WC.16.10.0007 |
| JL749A | Aruba 10G SFP+ LC LR 10km SMF TAA XCVR | WC.16.10.0007 |

**NOTE**

For information on networking application compatibility, see the Software Feature Support Matrix.

## YA/YB 16.11

This release applies to the following Aruba 2530 Switch Series:

**Table 6:** *Products Supported*

| Product number | Description |
|---|---|
| J9783A | Aruba 2530 8 Switch |
| J9782A | Aruba 2530 24 Switch |
| J9781A | Aruba 2530 48 Switch |
| J9777A | Aruba 2530 8G Switch |
| J9776A | Aruba 2530 24G Switch |
| J9775A | Aruba 2530 48G Switch |
| J9780A | Aruba 2530 8 PoE+ Switch |
| J9779A | Aruba 2530 24 PoE+ Switch |
| J9778A | Aruba 2530 48 PoE+ Switch |
| J9774A | Aruba 2530 8G PoE+ Switch |
| J9773A | Aruba 2530 24G PoE+ Switch |
| J9772A | Aruba 2530 48G PoE+ Switch |
| JL070A | Aruba 2530 8 PoE+ Internal Power Supply Switch |
| J9856A | Aruba 2530 24G 2SFP+ Switch |
| J9855A | 2530 48G 2SFP+ Switch |
| J9854A | 2530 24G PoE+ 2SFP+ Switch |
| J9853A | 2530 48G PoE+ 2SFP+ Switch |

# Minimum Supported Software Versions

If your switch or module is not listed in the below table, it runs on all versions of the software.

**Table 7:** *Minimum Supported Software Versions*

| Product number | Product name | Minimum software version |
|---|---|---|
| J9856A | Aruba 2530 24G 2SFP+ Switch | YA.15.15.0006 |
| J9855A | Aruba 2530 48G 2SFP+ Switch | YA.15.15.0006 |
| J9854A | Aruba 2530 24G PoE+ 2SFP+ Switch | YA.15.15.0006 |
| J9853A | Aruba 2530 48G PoE+ 2SFP+ Switch | YA.15.15.0006 |
| J9783A | Aruba 2530 8 Switch | YB.15.12.0006 |

| Product number | Product name | Minimum software version |
|---|---|---|
| J9782A | Aruba 2530 24 Switch | YB.15.12.0006 |
| J9780A | Aruba 2530 8 PoE+ Switch | YB.15.12.0006 |
| J9779A | Aruba 2530 24 PoE+ Switch | YB.15.12.0006 |
| J9781A | Aruba 2530 48 Switch | YA.15.12.0006 |
| J9778A | Aruba 2530 48 PoE+ Switch | YA.15.12.0006 |
| J9777A | Aruba 2530 8G Switch | YA.15.12.0006 |
| J9774A | Aruba 2530 8G PoE+ Switch | YA.15.12.0006 |
| J9776A | Aruba 2530 24G Switch | YA.15.10.0003 |
| J9775A | Aruba 2530 48G Switch | YA.15.10.0003 |
| J9773A | Aruba 2530 24G PoE+ Switch | YA.15.10.0003 |
| J9772A | Aruba 2530 48G PoE+ Switch | YA.15.10.0003 |

**NOTE**

For information on networking application compatibility, see the Software Feature Support Matrix.

## YC 16.11

This release applies to the following Aruba 2540 Switch Series:

**Table 8:** *Products Supported*

| Product number | Description |
|---|---|
| JL354A | Aruba 2540 24G 4SFP+ Switch |
| JL356A | Aruba 2540 24G PoE+ 4SFP+ Switch |
| JL355A | Aruba 2540 48G 4SFP+ Switch |
| JL357A | Aruba 2540 48G PoE+ 4SFP+ Switch |

This release note covers software versions for the 16.11 branch of the AOS-S software.

Version 16.11.0001 is the initial build of Major version 16.11 software. 16.11.0015 includes all enhancements and fixes in different versions of the 16.11 software.

Refer to the following topics for more information:

- Enhancements
- Fixes
- Issues and Workarounds

## Enhancements

This section lists enhancements added to this branch of the software.

Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

**Table 9:** *Enhancements*

| Version | Software | Switch | Description | Category |
|---------|----------|--------|-------------|----------|
| 16.11.0015 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | Support for removing old ciphers in the host key algorithm has been added. A new configuration option has been introduced which allows customers to remove **ssh-rsa** ciphers. Customers will be able to remove and disable outdated **ssh-rsa** ciphers in the host key algorithm using **ip ssh host-key-algorithm**. | SSH |
| 16.11.0015 | KB<br>WC | 5400R<br>2930F | Support to verify VSF error logs that are being sent to Central has been introduced. The **show logging** command can be used in the switch to verify VSF error events. | Central Integration |
| 16.11.0014 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | No enhancements were included in version 16.11.0014. | NA |
| 16.11.0013 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530 | No enhancements were included in version 16.11.0013. | NA |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
| | | 2540 | | |
| 16.11.0012 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | Support for https-based firmware downloads from Aruba Central has been added.<br>The firmware has been embedded with trust anchor for verifying the firmware repository server certificate. Updates are made to verify the Subject Alternative Name (SAN) from the server certificate and to limit the newly added trust anchor for only https-based firmware downloads. | Central Integration |
| 16.11.0011 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | No enhancements were included in version 16.11.0011. | NA |
| 16.11.0010 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | The User Role feature of the switch is enhanced to allow configuring the authentication client limits for a port.<br>The following new attributes are added under the device context of user role.<br><br>■ `client-limit dot1x` : Configure the 802.1X client-limit .<br><br>■ `client-limit mac-based`: Configure the mac-based client-limit on the client's port using the User Role.<br><br>When a client is authenticated with an user role with above attributes, the ports client limit is temporarily overridden.<br>Multiple overrides are allowed on same port using user role or RADIUS VSA, only if the new limits are greater than already applied limit. | User Role |
| 16.11.0009 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | Version 16.11.0009 is unavailable for download. | NA |
| 16.11.0008 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | No enhancements were included in version 16.11.0008. | NA |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
| 16.11.0007 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | A new configuration option is added in LLDP to mention which VLANs IP address should be included in the outbound LLDP advertisements of switch ports.<br>The IPv4/IPv6 address configured statically or dynamically assigned through DHCP on the specified management VLAN will be included in the outbound LLDP advertisements.<br>**Syntax:** `[no] lldp management-address vlan <vid>`<br><br>■ Interface level management address configuration will take precedence over the newly introduced management VLAN address.<br><br>■ In case of Multinetting, first IP address in the interface will be advertised.<br><br>■ Statically configured and dynamically assigned IP address of the LLDP management VLAN will be considered for advertising.<br><br>■ If the LLDP management VLAN has both IPv4 and IPv6 address configured, then both IPv4 and IPv6 address will be advertised.<br><br>■ If there is no IPv4 or IPv6 address present in the configured LLDP management VLAN, then the existing workflow will be used to select the management address.<br>Refer to the following documents for more information:<br>○ *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11*<br>○ *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11*<br>○ *Aruba 2530 Management and Configuration Guide for AOS-S 16.11*<br>○ *Aruba 2540 Management and Configuration Guide for AOS-S 16.11* | LLDP |
| 16.11.0007 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | To provide a secured management connection to the switch, the following improvements are made:<br>■ Disabled TELNET on default configuration (no telnet-server).<br>■ Disabled HTTP on default configuration (no web-management). | Security |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
| | | | ▪ Enabled HTTPS on default configuration (web-management ssl) using the installed self-signed certificate.<br><br>▪ Switch will redirect all HTTP request (including REST) to HTTPS, when HTTP is disabled and HTTPS is enabled.<br><br>The above configuration changes will be applied on firmware upgrade of switches with **default configuration**, i.e. only for switches that meet the following configuration criteria:<br><br>▪ Only the default VLAN must be present.<br><br>▪ The default VLAN should have DHCP IP rather than a static IP.<br><br>▪ AirWave should not be configured.<br><br>▪ Aruba Central URL should not be configured.<br><br>▪ Manger password should not be configured. | |
| 16.11.0006 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | The IP Auth manager feature has been added to close a TCP connection from an unauthorized client by sending a TCP RST immediately after receiving a TCP SYN packet, rather than allowing a complete three-way TCP handshake and then sending a TCP RST.<br><br>**NOTE:**<br>When an unauthorized client connects via the OOBM port, the existing behaviour remains unchanged. | Security |
| 16.11.0005 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | No enhancements were included in version 16.11.0005. | NA |
| 16.11.0004 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | OSPF Route Filtering feature provides an option to filter the intra-area routes from installing into local FIB table.<br>By using this, operator can create `distribute-list` with one or more network addresses which will be used to filter the intra area routes in OSPFv2/OSPFv3.<br>**Syntax:** | OSPF/OSPFv3 |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
|  |  |  | OSPFv2: `distribute-list <IP-ADDR>/<Prefix-Len>` <br><br> OSPFv3: `distribute-list <IPV6-ADDR>/<Prefix-Len>` <br><br> Refer to the following documents for more information: <ul><li>*Aruba 3810/5400R Multicasting and Routing Guide for AOS-S Switch 16.11*</li><li>*Aruba 3810/5400R IPv6 Configuration Guide for AOS-S Switch 16.11*</li><li>*Aruba 2930M/2930F Multicasting and Routing Guide for AOS-S Switch 16.11*</li><li>*Aruba 2930M/2930F IPv6 Configuration Guide for AOS-S Switch 16.11*</li></ul> |  |
| 16.11.0004 | KB <br> WC | 3810M <br> 5400R <br> 2930F <br> 2930M | Added support in Device fingerprinting (DFP) module to send protocol data to Aruba Central for telemetry. <br> Added `options-list` parameter to device-fingerprinting CLI. Switch software is enhanced to collect DHCP options list and up to three instances of HTTP user agent headers. <br> **Syntax:** `device-fingerprinting [policy]<PROFILE_NAME> dhcp [option-num <NUM> | options-list]`. <br> Refer to the following documents for more information: <br> *Aruba 3810/5400R Access Security Guide for AOS-S Switch 16.11* <br> *Aruba 2930M/2930F Access Security Guide for AOS-S Switch 16.11* | Device Finger Printing |
| 16.11.0003 | KB <br> WC | 3810M <br> 5400R <br> 2930F <br> 2930M | The Enrollment over Secured Transport (EST) client feature is updated to download and renew the CA certificates from an EST server independent of application certificate enrollment. A new command `est-server <profile-name>` <br> `cacerts-download` is added to enable independent CA certificate download from the EST server. This enhancement initiates automatic CA certificate download and renewal when the existing TA profile is about to expire. The switch will use the existing `est-server <profile-name>` <br> `re-enrollment-prior-expiry` command to determine how many days in advance the renewal is to be done. A MIB has also been added to enable automatic download and renew of the CA certificates from the EST server. | EST |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
| | | | Refer to the following documents for more information:<br>■ *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba MIB and Trap Support Matrix for AOS-S 16.11* | |
| 16.11.0002 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M | TCP timestamps are an extension to the original TCP stack, that was introduced to identify and reject old duplicate packets (PAWS) and to improve round-trip-time measurement. Using a scanner or other tool, an attacker can observe the TCP timestamp and determine the system uptime to gain information about the operational state of the system.<br>To avoid such risks, a new command `ip tcp randomize-timestamp` has been introduced to randomize the TCP timestamp offsets per connection. Once the command is issued, all the newly established TCP sessions will a use random offset along with the timestamp.<br>A MIB has also been added to enable or disable the randomization of TCP timestamp offsets.<br>Refer to the following documents for more information:<br>■ *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba 2530 Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba 2540 Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba MIB and Trap Support Matrix for AOS-S 16.11* | Security |
| 16.11.0002 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | This is an enhancement to an existing User-Based Tunneling `vlan-extend-enable` (VLAN-aware) mode. Silent devices like Programmable Logic Controller (PLC) devices do not initiate any traffic until they receive a message from the uplink server. Thus, such devices cannot leverage the benefits of colorless ports, which include being authenticated through a RADIUS server and being dynamically placed in a VLAN or being tunneled to a controller. | Support for Silent Device |

| Version | Software | Switch | Description | Category |
|---|---|---|---|---|
| | | | To support such silent devices, a new command `tunneled-node-server ubt-wol-enable vlan <VLAN-ID-LIST>` has been introduced. This command configures the silent client so that the controller allows the first packet from the silent server to reach the silent client without a user tunnel. This will initiate user authentication and tunnel formation.<br>A MIB has also been added to enable User-Based Tunneling Wake-on-LAN (WoL) on the specified VLANs.<br>Refer to the following documents for more information:<br>■ *Aruba 3810/5400R Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba 2930F/2930M Management and Configuration Guide for AOS-S 16.11*<br>■ *Aruba MIB and Trap Support Matrix for AOS-S 16.11* | |
| 16.11.0001 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | Updated all non-inclusive terminologies. Refer to Terminology Change for more information. | - |

# Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

**Table 10:** *Fixed Issues*

| Version | Bug ID | Software | Switch | Description | Category |
|---|---|---|---|---|---|
| 16.11.0015 | 257224<br><br>**NOTE:** Auto fixed by 257201. | WC | 2930F | **Symptom**: Customers reported SSH vulnerability alerts on the switch even after disabling CBC ciphers. The vulnerability scan reports the following: **The target is using deprecated SHA-1 cryptographic settings to communicate.** | SSH |

| Version | Bug ID | Software | Switch | Description | Category |
|---|---|---|---|---|---|
| | | | | **Scenario**: This issue occurred while running the vulnerability scanner which listed the weak host key algorithms supported in the switch. | |
| 16.11.0015 | 257206 | WC | 2930F | **Symptom/Scenario**: The switch interface went into an error state immediately after the upgrade. CRC error was noticed on the DAC VSF link after the upgrade. | VSF |
| 16.11.0015 | 257221 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch fails to stay in sync with Central.<br>**Scenario**: This issue occurred when ip igmp forward configuration pushed from Central did not get reflected in the switch. | Central Integration |
| 16.11.0015 | 257229 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom/Scenario**: The switch crashed immediately after configuring **logging filter <>** command options. | CLI |
| 16.11.0015 | 257233 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom/Scenario**: The message **Authentication is not triggered** appears both as debug log and throttled RMON log. | 802.1X |
| 16.11.0014 | 257001 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom/Scenario**: Cold/Warm start trap are not seen intermittently in the customer setup when the switch is cold/warm booted. | SNMPv3 |
| 16.11.0014 | 257076 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: Affected ports do not come with the LED blinking amber. Self test failure will be reported for the ports in the event log.<br>**Scenario**: This issue occurred when the switch or the line card was rebooted with some SPF+ ports having 1G transceivers.<br>**Workaround**: Reboot the switch or the reload the module. | Chassis Manager |
| 16.11.0014 | 257114 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Switch crashes with the following message: `Task='eDhcpv6Rly'`.<br>**Scenario**: This issue occured when the `dhcpv6 relay` command was configured with corrupted number of sockets causing the crash. | DHCP |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Workaround**: Disable the `dhcpv6 relay` command. | |
| 16.11.0014 | 257077 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: DHCP clients did not receive their IP addresses. The DHCP lease time is decremented to zero and is still available in the binding table.<br>**Scenario**: This issue occurred when multiple clients were connected to the server with a lease time of four minutes and ran the `dhcp client` command from the client device. | DHCP Snooping |
| 16.11.0013 | 257138 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: A configuration template push from Aruba Central fails.<br>**Scenario**: This issue occurred when the configuration template is updated to `dhcp-snooping vlan <vlanid rnage>` from `dhcp-snooping vlan <vlan>`. | Central Integration |
| 16.11.0013 | 257136 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch sends cold start trap instead of warm start trap after rebooting.<br>**Scenario**: This issue occurred when the switch was rebooted with the boot `system/reload/reboot` command. | SNMPv3 |
| 16.11.0013 | 257133 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Switch crashes with the following error message:<br>`Software exception at vls_xmit.c:161 – in 'mBonjourCtrl'`<br>**Scenario**: This issue occurred when an MDNS profile was configured with a corrupted MDNS packet causing the crash. | Boot and Reload |
| 16.11.0013 | 257122 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: The client MAC address remains in the Port Access MAC-Based Client Session Table even when the client moves to a different switch. This leads to reaching the maximum limit of 256 authentications and prevents further MAC authentications.<br>**Scenario**: This issue occurred when MAC authentication was configured on the switch and the PVLAN isolated client was moved from one switch to another switch. | MAC Authentication |
| 16.11.0013 | 257104 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: OSPFv3 is not acknowledging specific LSU updates.<br>**Scenario**: This issue occurred when two switches were connected with OSPFv3 enabled and one switch acted as an ABR sending LSU Type 4 containing router LSA with a non-zero LS ID. | OSPFv3 |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0013 | 257105 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Switch fails to move to initial role when connectivity to the RADIUS server is lost.<br>**Scenario**: This issue occurred when the clients were authenticated with user roles attributed with port-mode and when the RADIUS server connectivity became unreachable.<br>**Workaround**: Toggle the port. | User Role |
| 16.11.0013 | 257091 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: UBT user traffic will not get tunneled.<br>**Scenario**: This issue occurred when a MAC move of UBT users from one port to another was initiated.<br>**Workaround**: Disable and enable the feature using `no tunneled-node-server enable` and `tunneled-node-server enable` commands. | Tunneled Node |
| 16.11.0013 | 257073 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Some DHCP client's DHCP offers are dropped by DHCP snooping.<br>**Scenario**: This issue occurred when the server pool is configured with different subnet masks wider than /24 and when the client requests an unicast DHCP offer packet.<br>**Workaround**: Configure multiple ranges in the pool excluding the following IP addresses:<br>■ x.x.x.255<br>■ x.x.x.0 | DHCP Snooping |
| 16.11.0013 | 257089 | YA/YB<br>YC | 2530<br>2540 | **Symptom**: Some switches are unable to connect to Aruba Central. The switch crashed with the following error message:<br>`Internal error : HTTP/1.1 protocol missing. Please contact Aruba support.`<br>**Scenario**: This crash occurred due to a rare timing issue.<br>Workaournd: Disable and enable Aruba Central. | Central Integration |
| 16.11.0013 | 257089 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Some switches are unable to connect to Aruba Central. The switch crashed with the following error message:<br>`Internal error : HTTP/1.1 protocol missing. Please contact Aruba support.`<br>**Scenario**: This crash occurred due to a rare timing issue.<br>Workaournd: Disable and enable Aruba Central. | Central Integration |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0013 | 257088 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: A configuration template push of `timesync` with `ntp` from Aruba Central fails.<br>**Scenario**: This issue occurred when `timesync <>` configuration was pushed from Aruba Central when NTP was enabled. | Central Integration |
| 16.11.0013 | 257082 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: NTP server authentication fails in Aruba Central.<br>**Scenario**: This issue occurred when the NTP key was validated with `encrypt-credential` enabled in Aruba Central.<br>**Workaround**: Reboot the switch after pushing the configurations. | NTP |
| 16.11.0013 | 257070 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch crashed and reboots while accessing the WebUI.<br>**Scenario**: This issue occurred when LLDP packets were sent with a system name TLV length of 255 by neighbour device.<br>**Workaround**: Disable LLDP on the port which is connected to a device sending LLDP packets with the values mentioned above. | LLDP |
| 16.11.0013 | 257063 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The output of the command `show power-over-ethernet <port>` displays **PD Power Draw** value in decimals while the corresponding REST API truncates it to a whole number.<br>**Scenario**: This issue occurred when the REST API GET /ports/<port>/poe/stat command was configured. | REST API |
| 16.11.0013 | 257049 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Manager or operator credentials are lost after rebooting the switch.<br>**Scenario**: This issue occurred when the command `include-credentials` was enabled and the switch was power cycled.<br>**Workaround**: Save the switch configuration details after enabling `include-credentials`. | Credentials |
| 16.11.0012 | 256928 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: The interface module of the switch crashes with either of the following signatures.<br>■ `Ports 1-24,A subsystem went down: 12/15/22 08:31:08 KB.16.10.0020 646Software exception in kernel context at ghsException.c:1539-> Internal system error at 0x869e034` | Flex Port |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | ■ Ports 1-24,A subsystem went down: 12/11/22 02:42:10 KB.16.10.0020 646Health Monitor: Write Error Restr Mem AccessHW Addr=0xc04e1c18 IP=0x882bfbc Task='mPmSlvCtrl' Task ID=0x6bce41c0Bus Err Data=0x00000000 Bus Err Status=0x100008d1 Status=0xb0000001 Bus Err Addr=0xec020f4<br><br>■ Ports 9-16 subsystem went down: 12/08/22 01:09:01 KB.16.10.0020 646Health Monitor: Read Error Restr Mem AccessHW Addr=0xe0200410 IP=0x8800c74 Task='mIpAdMUpCt' Task ID=0x6bccc140Bus Err Data=0x00000000 Bus Err Status=0x100008d1 Status=0xb0000001 Bus Err Addr=0xec02f540 | |
| 16.11.0012 | 257080 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: VSF switch stack connected to Aruba Central crashes.<br>**Scenario**: This crash is a rare scenario and occurred when one of the switch members was not able to collect the temperate data. | Central Integration |
| 16.11.0012 | 257033 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: The switch logs the event :Unsolicited Echo Reply from <ip address>.<br>**Scenario**: This issue occurred when the DHCP server was enabled in the switch and the DHCP client connected to the switch for the first time. | DHCP |
| 16.11.0012 | 257023 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: amp-server secret is not encrypted even after configuring encrypt-credentials.<br>**Scenario**: This problem occurred when the amp-server secret was configured, followed by encrypt-credentials, but the amp-server secret was not encrypted and appeared as plain-text under show running-config. | Config |
| 16.11.0012 | 257031 | KB WC YC | 3810M 5400R 2930F 2930M | **Symptom**: Switch crashes due to invalid memory access.<br>**Scenario**: This issue occurred when the switch sent DFP data to Cisco ISE. | Device Finger Printing |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | 2540 | **Workaround**: Configure the valid ClearPass IP address and credentials in the switch. | |
| 16.11.0012 | 257005 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: SSH session from the switch to AP505 does not close sometimes when the exit command is executed. **Scenario**: This issue occurred when the SSH session is established from the switch to AP 505. execute the command exit. **Workaround**: Use the key sequence ~. | SSH |
| 16.11.0012 | 257023 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: amp-server secret is not encrypted even after configuring encrypt-credentials. **Scenario**: This problem occurred when the amp-server secret was configured, followed by encrypt-credentials, but the amp-server secret was not encrypted and appeared as plain-text under `show running-config`. | Config |
| 16.11.0012 | 257005 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: SSH session from the switch to AP505 does not close sometimes when the exit command is executed. **Scenario**: This issue occurred when the SSH session is established from the switch to AP 505. execute the command exit. **Workaround**: Use the key sequence ~. | SSH |
| 16.11.0011 | 256897 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: The switch crashes with the message similar to `Software exception in ISR at Interrupts_fd.c:1145 -> Excessive FD 0 interupts`. **Scenario**: This issue occurred when the IPSEC traffic was tunneled via UBT. | Tunneled Node |
| 16.11.0011 | 256956 | KB | 3810M 5400R | **Symptom**: An incorrect community string is advertised from a neighbor AOS-S switch. **Scenario**: This issue occurred when the BGP community string with more than 3 digits was set in the format AS:NN on a KB platform switch and advertised to neighbor. **Workaround**: Use a shorter community string. | BGP |
| 16.11.0011 | 256927 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: The devices that are not directly connected to the switch show up in the LLDP neighbour table. **Scenario**: This issue occurred when the device sent LLDPDUs with the STP multicast destination MAC address and STP was disabled in the switch. | LLDP |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Workaround**: Configure an ACL on the interface connected to the device to drop the packets with STP multicast destination MAC address. | |
| 16.11.0011 | 256958 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The top interface metric is empty in the dashboard page of WebUI.<br>**Scenario**: This issue occurred when the WebUI was accessed 18 times or more with the duration of each access lasting more than a minute.<br>**Workaround**: Reboot the switch. | WebUI |
| 16.11.0011 | 256991 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: The switch fails to come online.<br>**Scenario**: This issue occurred when the `netservice` and `netdestination` was configured with `ip access-list` on the switch.<br>**Workaround**: Remove the `netservice` configuration. | Management Stacking |
| 16.11.0011 | 256995 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Unable to get the LAG MIB information through SNMP in the operator mode.<br>**Scenario**: This issue occurred when the LACP and SNMP server community were configured in the operator mode and SNMP Walk was performed. | SNMPv2 |
| 16.11.0011 | 256987 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch crashes while connecting to Aruba Central.<br>**Scenario**: This issue occurred when the switch running AOS-S16.07 or older version was upgraded to AOS-S 16.08 or a later version and attempted to connect to Aruba Central. This issue has a very low probability of occurrence.<br>**Workaround**: Power cycle the switch one more time after the upgrade. | REST Infrastructure |
| 16.11.0011 | 256905 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch passwords are not erased after `erase all` command is executed.<br>**Scenario**: This issue occurred when the passwords were configured on the switch and then the `erase all` command was executed.<br>**Workaround**: Execute `no password manager/no password operator` commands prior to the `erase all` command. | Credentials |
| 16.11.0011 | 256876 | KB | 3810M<br>5400R | **Symptom**: HTTP traffic from clients does not pass through UBT. | Device Finger Printing |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Scenario**: This issue occurred when the UBT topology with device finger-printing was enabled on the switch. Device finger-printing must include HTTP protocol.<br>**Workaround**: Disable device finger-printing. | |
| 16.11.0010 | 256816 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Some of the data displayed in the `show system power-supply detail` command output, such as `AC MAIN Voltage` and `Power Supplied` may be incorrect for some JL087A model PSUs.<br>**Scenario**: This issue occurred when some of the JL087A model PSUs were powered on and the `show-system power-supply` command was executed and the output parameters like Voltage and Power were out of range.<br>**Note:** This is an issue with the command output only and doesn't impact the PSU functionality. | Chassis Manager |
| 16.11.0010 | 256676 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: The PSU is operational and delivering power, even though the status is displayed as `Faulted` in some PSU/PoE related `show` commands.<br>**Scenario**: This issue occurred when the PSU fan had a failure and the PSU/PoE related `show` commands were executed.<br>**Note:** PSU may be operational in this scenario although the related `show` commands indicate a fault. If the operating temperature is no longer ambient for PSU, it will shut down and the PSU operational state will match the output of the `show` command. | Chassis Manager |
| 16.11.0010 | 256679 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Switch event logs will not be generated even if PSU encounters multiple problems like over temperature, over current, fan fault, and so on.<br>**Scenario**: This issue occurred when there was a recurring set of one or more PSU events, such as overcurrent, overheating, and so on. However, such events are not anticipated in most of the deployments. | Chassis Manager |
| 16.11.0010 | 256651 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: System memory depletes and the switch reboots after a few months of runtime. | Central Integration |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Scenario**: This issue occurred when the switch was connected to AirWave, and the AirWave was polling certain MIBs including `ieee8021SpanningTreeDesignatedRoot` and `hpicfXpsSwitchModType`. | |
| 16.11.0010 | 256812 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The simultaneous execution of `Show Tech` from the switch CLI and from Aruba Central may cause the switch to crash.<br>**Scenario**: This issue occurred when the user executed the `Show Tech` command in CLI and Aruba Central in parallel. | Boot and Reload |
| 16.11.0010 | 256872 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The switch crashes with the message similar to:`NMI event SW:IP=0x0ea80030 MSR:0x02029200 LR:0x0ea800cccr: 0x42000400 sp:0x1f5d46e8 xer:0x00000000Task='mDsnoopCtrl' Task ID=0x1f5d13a8`.<br>**Scenario**: This issue can occur if the DHCP snooping is enabled and the switch is processing continuous DHCP packets.<br>**Workaround**: Disable the DHCP snooping. | DHCP Snooping |
| 16.11.0010 | 256887 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: The switch management module crashes.<br>**Scenario**: This issue occurred when the switch was configured with an initial role containing a `reauth-period`. The mac-auth clients were placed in the initial role as the controller was not reachable. Later, the controller connectivity was regained within the time window of the mac-auth client re-authentication. | Coredump |
| 16.11.0010 | 256860 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: The switch will run out of ternary content addressable memory (TCAM) meter resources and the client authentication using user roles fails.<br>**Scenario**: This issue occurred when the last port with DFP config was toggled for several times. | Device Finger Printing |
| 16.11.0010 | 256898 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Authentication fails due to an insufficient ACL resources error.<br>**Scenario**: This issue occurred when the client was authenticated using a user role with a classifier configuration having a VLAN which was not configured on the switch. | Access Control Lists (ACL) |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Workaround**: Make sure that the VLANs used in classifier configuration is present in the switch. | |
| 16.11.0010 | 256935 | YA/YB YC | 2530 2540 | **Symptom**: The switch crashed with a message similar to `Software exception at wma_ctrl_sm.c:283 – in 'mWebAuth'.`<br>**Scenario**: This issue occurred when the `User Role`, `Auth order`, and `Server timeout` were configured on the switch, and RADIUS server was unreachable. | Mac Authentication |
| 16.11.0009 | - | KB | 3810M 5400R | Version 16.11.0009 is unavailable for download. | - |
| 16.11.0008 | 256574 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: The switch crashes if the `ip tcp randomize-timestamp` configuration is present on the switch.<br>**Scenario**: This issue occurred when the switch had the `ip tcp randomize-timestamp` configuration and SSH/Telnet/Web UI was established on the switch.<br>**Workaround**: Remove the `ip tcp randomize-timestamp` configuration. | Boot and Reload |
| 16.11.0008 | 256762 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: The switch configuration fails with an `invalid oobm` or `400 bad response` error when the RADIUS server is updated with `is_oobm` or `is_tls_oobm` and the value is updated from `False` to `False`.<br>**Scenario**: This issue occurred when the PUT request was sent to the RADIUS server with `is_oobm` or `is_tls_oobm` and the value was updated from `False` to `False` (no change). | REST APIs |
| 16.11.0008 | 256800 | KB | 3810M 5400R | **Symptom**: Clients experience random connectivity issues in a topology with the distributed trunking (DT) switches because connected devices' MAC addresses are learned on the inter switch connect (ISC) ports.<br>**Scenario**: This issue occurred when the DT switches were not connected (inter switch connect) via a direct layer 1 connection, and ISC port flaps on either of the DT switches.<br>**Workaround**: Clear MAC address on both the DT switches. | Distributed Trunking |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0008 | 256727 | WC | 2930F 2930M | **Symptom/Scenario**: The switch crashes when the OSPF neighbor sends exactly 256 OSPF routes. **Workaround**: Configure the OSPF protocol with more or less than 256 OSPF routes. | OSPF |
| 16.11.0007 | 256543 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: IPTV stream freezes on a periodic basis as the querier information is lost. **Scenario**: This issue occurred when IGMPv3 query was sent with a QQIC value lower than IGMPv2 config. **Workaround**: Change the querier interval value configured for IGMPv2 to a value higher than 60 seconds (default IGMPv2 querier interval). | IGMPv3 |
| 16.11.0007 | 256613 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom/Scenario**: Some IP addresses for `save config` and `config change` in the traps will not be displayed in the AirWave. | AirWave |
| 16.11.0007 | 256631 | KB WC | 3810M 5400R 2930F 2930M | **Symptom/Scenario**: UBT Client on one port will authenticate and a tunnel is established, but no traffic passes and the counter `packets to non existent tunnel` will increase. Other ports may function normally. **Workaround**: `Disable` or `Enable` either the tunneled-node-profile or the UBT user port. | Tunneled Node |
| 16.11.0007 | 256695 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: Dynamically learned routes will lose the nexthop and traffic will not be forwarded. **Scenario**: This issue occurred when VRRP was configured in owner mode along with routing protocols. **Workaround**: Configure VRRP in backup mode when using routing protocols. | OSPFv2 |
| 16.11.0007 | 256733 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: IP SLA for reachability failed status shows garbage RTT value when polling using SNMP, i.e. `hpicfIpSlaHistSummRTT` returns non zero values even for unreachable history records. **Scenario**: This issue occurred when the IP SLA target was reachable for 25 intervals and then became unreachable. | IP SLA |
| 16.11.0007 | 256575 | KB WC | 3810M 5400R | **Symptom**: The switch stops responding to valid SNMP packets. | SNMPv3 |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | YA/YB YC | 2930F 2930M 2530 2540 | **Scenario**: This issue occurred when the UDP packets were sent without any data. After 65 packets, the switch will stop responding to valid packets. | |
| 16.11.0007 | 256600 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: Client will not be in authenticated state until cached-reauth period.<br>**Scenario**: This issue occurred when the 802.1x authentication was configured with the cached-reauth.<br>**Workaround**:<br>■ First, enable the user-role authentication and then configure the critical user-role for the authentication port.<br>■ Critical user-role should not have the reauth-period attribute and auth-order should be removed for the authentication port. | 802.1x |
| 16.11.0007 | 256732 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: Local-user with group cannot be configured via SNMP.<br>**Scenario**: This issue occurred when the local-user with group using SNMP was configured.<br>**Workaround**: User can configure local-user with group using CLI configuration. | SNMPv2 |
| 16.11.0007 | 256672 | YA/YB | 2530 | **Symptom/Scenario**: The switch fails to connect to activate with an error `activate: EST enrollment with server failed because of Unable to generate CSR.` | Central Integration |
| 16.11.0006 | 256590 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom/Scenario**: When a port is added to a VLAN from the Web UI, IPv6 will be enabled on the VLAN. | NextGen WebUI |
| 16.11.0006 | 256541 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: **Authentication** or **Accounting** using RadSec server is delayed.<br>**Scenario**: This issue occurred when there was only one RadSec server configured and the TLS connection to that server was terminated. | Radius |
| 16.11.0006 | 256509 | KB WC | 3810M 5400R 2930F | **Symptom**: The BSR and RP candidate cannot be configured with a VLAN ID greater than 999. | PIM Sparse Mode |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | 2930M | **Scenario**: This issue occurred when a VLAN ID greater than 999 was configured with `ip pim-sparse` enabled and `bsr-candidate`/`rp-candidate` was configured in `router pim/pim6` with the respective VLAN ID. | |
| 16.11.0006 | 256491 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: Multicast traffic stops for several seconds, causing the video stream to freeze. **Scenario**: This issue occurred when multiple clients were connected to the same access switch (the access layer with AOS-S switches and distribution/core layer with CX switches) receiving the same multicast stream, and one of the clients sent an IGMP leave. This fix is only specific to IGMPv2. | IGMP |
| 16.11.0006 | 256485 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: REST request over HTTPS fails as SSL connection is not established. **Scenario**: This issue occurred when a GET request with an empty JSON payload was sent. **Workaround**: Replace the empty JSON payload with *None* in the GET request. | REST APIs |
| 16.11.0006 | 256372 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: Traffic from the secondary VLAN does not reach the primary VLAN. **Scenario**: This issue occurred when there was a tagged trunk port in the secondary VLAN and the switch was rebooted. **Workaround**: Remove the tagged trunk configuration from the secondary VLAN and re-add the tagged trunk configuration to the secondary VLAN. | PVLAN |
| 16.11.0006 | 256358 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: An invalid username or password grants the operator access to the switch's Web UI. **Scenario**: This issue occurred when a banner and a manager password were configured but not an operator password. **Workaround**: Remove the banner configuration. | WEB UI |
| 16.11.0006 | 256561 | YA/YB | 2530 | **Symptom**: Network access is denied for a 802.1X authenticated client. **Scenario**: This issue occurred when the 802.1X client was authenticated with the `auth-vid` and `unauth-vid` configurations. **Workaround**: Configure a client limit for the authenticator-enabled port. | 802.1X |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0005 | 256433 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: When an end client is moved between two different switches, authentication does not occur on the second switch. **Scenario**: This issue occurred when the MAC address of the end client is learned on the uplink port first (where authentication was not enabled) and later learned on an access port (where authentication was enabled). | Mac Authentication |
| 16.11.0005 | 256424 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: Device fingerprinting fails when the first RADIUS server in the list is unreachable. **Scenario**: This issue occurred when there were more than one RADIUS server configured and the first server in the list was not reachable. **Workaround**: Keep the unreachable RADIUS server as the last entry in the list. | Device Finger Printing |
| 16.11.0005 | 256420 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom/Scenario**: The switch crashes after entering the `ip-recv-mac-address` command. **Workaround**: Use an interval value greater than 2 when configuring `ip-recv-mac-address`. | Boot and Reload |
| 16.11.0005 | 256406 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: Traffic is sent directly to clients in VLANs that do not have an IP address configured instead of being sent to the gateway configured in the routing table. **Scenario**: This issue occurred when the switch had both Layer 2 and Layer 3 VLANs and IP client tracker was enabled. **Workaround**: Disable the IP client tracker. **Note:** The IP address of silent clients being tracked may not be learnt unless a port bounce is performed after a redundancy failover. | Static Routing |
| 16.11.0005 | 256366 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom/Scenario**: The switch crashes with a message similar to the following: `Software exception at multMgmtUtil.c:259 – in 'mOobmCtrl' -> Internal error.` | Coredump |
| 16.11.0005 | 256349 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: The memory of the switch is slowly consumed until executing any CLI command results in an `Out of memory` message. **Scenario**: This issue occurred when the switch had `aaa` configured, was connected to Aruba Central, and had neighbours that shared LLDP information. | VSF |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0005 | 256122 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: Tx drops are seen on the port after the trunk member is removed.<br>**Scenario**: This issue occurred when the port was configured to be a member of the trunk and subsequently removed from the trunk when the port was down. The issue will be seen when a client is connected to the port.<br>**Workaround**: Configure the trunk while the port is up. | LACP |
| 16.11.0005 | 256069 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: The switch reports a selftest failure on transceiver ports with `Rx timeout` error.<br>**Scenario**: This issue occurred when the 3810 stack rebooted with SFP+ flex modules and J8177D transceivers. | Chassis Manager |
| 16.11.0005 | 256301 | WC | 2930F<br>2930M | **Symptom**: The port is mistakenly blocked by MACsec.<br>**Scenario**: This issue occurred when MACSec was configured and the switch was up for approximately 100 days. | Mac_Sec |
| 16.11.0005 | 256262 | WC | 2930F<br>2930M | **Symptom**: Delay in captive portal redirection.<br>**Scenario**: This issue occurred when multiple clients were connected and when there were several TLS sessions from each client. | Captive Portal |
| 16.11.0005 | 256247 | WC | 2930F<br>2930M | **Symptom/Scenario**: The stack topology shown in the `show stacking` output is Chain even though the actual topology is a Ring. | Back Plane Stacking |
| 16.11.0004 | 256202 | YA/YB | 2530 | **Symptom**: Unable to provision the switch from Aruba Activate and records an EST enrollment failure.<br>**Scenario**: This issue occurred when the hostname for the EST enrollment server is not resolved during zero-touch provisioning (ZTP).<br>**Workaround**: Ensure that the DHCP server provides a DNS server IP address. | CertManager |
| 16.11.0004 | 256274 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom/Scenario**: `VSF` Stack Member crashed with a message similar to the following:<br>`Software exception at lava_`<br>`chassis_slot_sm.c:3626 – in`<br>`'eChassMgr', task ID =`<br>`0x37b07bc0.` | VSF |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0004 | 256257 | KB YA/YB YC | 3810M 5400R 2530 2540 | **Symptom/Scenario**: Certain transceivers had link issues in unsupported transceiver mode. | Transceivers |
| 16.11.0004 | 256234 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: The `show rmon statistics <port no>` command returns the wrong counter values.<br>**Scenario**: This issue occurred when the `clear statistics global` or `clear statistics <port no>` was executed first and then `show rmon statistics <port no>`. | CLI |
| 16.11.0004 | 256233 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: Client ports may encounter packet drops when multicast sources stream video over 500 Mbps.<br>**Scenario**: This issue can occur when multiple clients from different ports subscribed to the same group, which streams using HD channels requiring high bandwidth. TX drops can occur when several clients change channels simultaneously.<br>**Workaround**: Lower the bandwidth of the video streams to below 500 Mbps in order to avoid over-subscription of ports. | IGMP-NG |
| 16.11.0004 | 256220 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: Missing OSPF routes.<br>**Scenario**: This issue occurred when both userbased tunneling and OSPF are configured and either of the uplinks to the controller is down.<br>`source-interface` to be configured for tunneled node when the switch has more than one vlan to the reach the controller. | OSPFv2 |
| 16.11.0004 | 256205 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: A configuration template push from Aruba Central fails.<br>**Scenario**: This issue occurred when the end devices are connected to ports that are configured with `port-security learn-mode static`. | Central Integration |
| 16.11.0004 | 256121 | KB WC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: Web authentication fails when the switch is managed by Aruba Central (aruba-central support-mode disable).<br>**Scenario**: This issue occurred when the switch connects to Aruba Central and `aruba-central support-mode` is disabled.<br>**Workaround**: Execute `aruba-central support-mode enable` command so the switch is no longer managed by Aruba Central. | Web Authentication |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0004 | 256140 | KB | 3810M<br>5400R | **Symptom**: The switch crashes with an error message: `NMI event`.<br>**Scenario**: This issue occurred when the HP MSM 775 wireless controller was connected to the switch and `snmpwalk` was executed. | SNMPV2 |
| 16.11.0004 | 256167 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Ports with per-port tunneled node (PPTN) configured may be disabled after a switch reboot.<br>**Scenario**: This issue occurred when a device profile was configured with tunneled-node.<br>**Workaround**: Disable and enable the problematic PPTN enabled port manually. | Tunneled Node |
| 16.11.004 | 256144 | KB | 3810M<br>5400R | **Symptom**: The switch is unable to establish a connection with Aruba Activate.<br>**Scenario**: This issue occurred when the switch was first onboarded, but it can also happen after the switch is visible on Aruba Central. | Activate |
| 16.11.0004 | 255916 | KB | 3810M<br>5400R | **Symptom/Scenario**: Slot crashes with signatures `OMFP LPTR Err Status = 0x00000310 (DEC_ERR_CNT)` and `FR Error = 0x18000020 (ALLOC_CHIP_PORT_UNDERFLOW)`. | Basic Layer2 |
| 16.11.0004 | 256115 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Although the switch does not react to pings or SSH commands, it continues to transit traffic. The event log contains a crash message.<br>**Scenario**: This issue occurred when device fingerprinting was configured with DHCP protocol. | CPPM |
| 16.11.0003 | 256037 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: Clients are not authenticated on a switch port.<br>**Scenario**: This issue occurred when multiple clients were connected to a single port (for example, a Personal Computer (PC) was connected to a phone), both MAC authentication and 802.1X authentication methods were attempted at the same time on the PC, and both the authentication methods used the same user role attribute.<br>**Workaround**: Configure the `auth-order` parameter first with `authenticator`, and then with `mac-based`. | 802.1X |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0003 | 255940 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception at svc_ misc.c:1088 – in 'mDHCPClint'`<br>`-> Failed to malloc 9202 bytes`<br>**Scenario**: This issue occurred when the switch attempted to reconnect to Aruba Central. | Aruba Central |
| 16.11.0003 | 255928 | KB WC YC | 3810M 5400R 2930F 2930M 2540 | **Symptom/Scenario**: A switch is unable to connect to Aruba Central. | Aruba Central |
| 16.11.0003 | 255978 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: A switch crashes with a message similar to the following:<br>`Software exception in ISR at pvDmaV1Rx.c`<br>`-> ASSERT: No resources available!`<br>**Scenario**: This issue occurred when 802.1X and MAC authentication were enabled on the same port with auth-order, and the client was initially authenticated through MAC authentication with a user role having the `port mode` attribute. | Authentication |
| 16.11.0003 | 255896 | KB | 3810M 5400R | **Symptom**: A stack member loses connection to the stack and gets stuck in a boot loop.<br>**Scenario**: This issue occurred when the stacking links were configured as a full mesh, and two links went down leaving the stacking links in a chain configuration. | Back Plan Stacking |
| 16.11.0003 | 256123 | KB | 3810M 5400R | **Symptom**: Received packet drops are observed on a port.<br>**Scenario**: This issue occurred when the TCP traffic, with the push flag set, consumed 100% bandwidth on a 1G port of a V3 module. | Interfaces |
| 16.11.0003 | 255995 | KB YC YA/YB YC | 3810M 5400R 2930F 2930M 2530 2540 | **Symptom**: A switch crashes when the `show port-access clients` command is issued or when an `SNMP GET` operation is performed to get the MIB object `hpicfUsrAuthMacAuthSessionStatsE ntry`. | Authentication |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | |
| 16.11.0003 | 255120 | YA/YB | 2530 | **Symptom/Scenario**: The Key Expansion Module of a Cisco 8851 phone does not power up.<br>**Workaround**: Configure `poe-allocate-by` command with `class` parameter on the ports, and reduce the number of powered devices connected to the switch. | PoE |
| 16.11.0003 | 255819 | YA/YB | 2530 | **Symptom**: A switch crashes with a message similar to the following:<br>`SubSystem 100 went down:`<br>`Health Monitor: Read Error Restr`<br>`Mem Access`<br>**Scenario**: This issue occurred because of the following actions:<br>1. An AP was authenticated with 802.1X `port mode`.<br>2. The AP was rebooted, and the 802.1X authentication configuration was removed from the port. | 802.1X |
| 16.11.0003 | 256016 | KB<br>WC<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2540 | **Symptom**: When a private VLAN is configured on a switch, the traffic from the secondary VLAN does not reach the primary VLAN.<br>**Scenario**: This issue occurred when the switch was rebooted, and the secondary VLAN contained a tagged trunk or Link Aggregation Control Protocol (LACP) port.<br>**Workaround**: Remove and add the tagged trunk or LACP configuration to the secondary VLAN. | Private VLAN |
| 16.11.0003 | 254566 | KB<br>WC | 3810M<br>5400R<br>2930F<br>2930M | **Symptom**: Traffic fails to pass through an IEEE 802.1ad tunnel.<br>**Scenario**: This issue occurred because of the following reasons:<br>1. A Small Form-factor Pluggable+ (SFP+) port was configured as an uplink.<br>2. IEEE 802.1ad was configured on the same port.<br>3. The switch was rebooted without a transceiver in the slot.<br>4. A 1G SFP transceiver was inserted during the runtime. | IEEE 802.1ad |

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| | | | | **Workaround**: Insert the 1G SFP transceiver, and then reboot the switch. | |
| 16.11.0003 | 256034 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: SNMP MIB files are not reachable, and the MIB file returns some errors.<br>**Scenario**: This issue occurred when the customer used an SNMP monitoring tool to read or parse the MIB files. | SNMP |
| 16.11.0003 | 256050 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: A switch crashes when the **WebUI Security > Clientspage** is accessed.<br>**Scenario**: The switch crashed when a MAC-authenticated client had a username of more than 40 characters. | Web UI |
| 16.11.0002 | 255888 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom/Scenario**: When a proxy server is configured on the switch, the switch does not onboard into Aruba Central or Activate. | Aruba Central |
| 16.11.0002 | 255799 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom**: The user is unable to copy a configuration file to the switch using Secure File Transfer Protocol (SFTP) and the following error message is displayed. Invalid input: grep usage error<br>**Scenario**: This issue occurred when the pipe character ( \| ) was used as a part of the command input for some configuration commands, such as the `banner motd` and `snmpv3 user` commands.<br>**Workaround**: Do not use the pipe character (\|) in the command input for the configuration commands. | Configuration |
| 16.11.0002 | 255825 | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | **Symptom/Scenario**: When a switch is rebooted through an SSH session, the `show boot-history`, `show logging`, and `boot` command outputs include the `Operator cold reboot from TELNET session` message instead of the `Operator cold reboot from SSH session` message. | SSH |
| 16.11.0001 | - | KB<br>WC<br>YA/YB<br>YC | 3810M<br>5400R<br>2930F<br>2930M<br>2530<br>2540 | No fixes were included in version 16.11.0001. | - |

# Issues and Workarounds

The following are known open issues with this branch of the software.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue.

**Table 11:** *Known Issues*

| Version | Bug ID | Software | Switch | Description | Category |
|---------|--------|----------|--------|-------------|----------|
| 16.11.0010 | 256986 | KB WC | 3810M 5400R 2930F 2930M | **Symptom/Scenario**: UBT Client on one port will authenticate and a tunnel is established, but no traffic passes and the counter `packets to non existent tunnel` will increase. Other ports may function normally. **Workaround**: `Disable` or `Enable` either the tunneled-node-profile or the UBT user port. | Tunneled Node |
| 16.11.0006 | 256681 | KB WC | 3810M 5400R 2930F 2930M | **Symptom**: Loop protect does not block the PBT enabled port in tunnel established/establishing state. **Scenario**: This issue occurred when the loop protect was enabled or configured for a PBT-enabled port in the tunnel-established state. **Workaround**: Disable or enable PBT for the affected ports. **NOTE:** When using PBT, it is recommended to use STP instead of loop protect. If inevitable, loop protect must be enabled first and then the PBT on the port. | Tunneled Node |

# Upgrade Information

This chapter provides upgrading restrictions and guidelines for the following software platforms:

- KB 16.11
- WC 16.11
- YA/YB 16.11
- YC 16.11

# KB 16.11

KB.16.11.0015 uses BootROM KB.16.01.0006 when running on 5400R switches and BootROM KB.16.01.0008 when running on 3810M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

Some units of 5400R and 3810M switches may have BootROM version KB.16.01.0009 already and it remains unaffected.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.01 is not allowed if MSTP instances configured are greater than 16; or the max-vlans value is greater than 2048, or this system is part of a VSF stack.

Unconfigure these features before attempting to downgrade from KB.16.01.0004 or later to a version earlier than 16.01 of the firmware.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

# WC 16.11

WC.16.11.0015 uses BootROM WC.16.01.0010 when running on 2930F switches and BootROM WC.17.02.0007 when running on 2930M switches. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.
IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of theBasic Operation Guide.

## YA/YB 16.11

YA/YB.16.11.0015 uses BootROM YA.15.20/YB.15.10. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the **Basic Operation Guide**.

## YC 16.11

YC.16.11.0015 uses BootROM YC.16.01.0003. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

IMPORTANT: During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

Firmware downgrade to a version earlier than 16.04 will generate new SSH keys upon switch boot-up. These keys will be different than the ones previously stored in SSH peer's known hosts file and may result in SSH connectivity issues after the OS downgrade completes. You will need to erase the pre-existing switch keys from SSH peer's known hosts file to restore SSH connectivity.

This issue will not be encountered when the option "StrictHostKeyChecking" is disabled in the SSH peer.

For more information regarding clearing SSH keys and changing strict host key checking settings, see the documentation provided with your SSH client.

For information on best practices when updating software or rolling back to previous versions of software, see the "Best practices for software updates" section of the Basic Operation Guide.

## Aruba Security Policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.

- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/sirt/.
Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/security-bulletins/.