AOS-CX 10.12.0006 Release Notes

9300 Switch Series

a Hewlett Packard
Enterprise company

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Products Supported

This release applies to the 9300Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

NOTE

If your product is not listed in the below table, no minimum software version is required.

Product number	Product name	Minimum software version
R9A29A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Front-to-Back 6 Fans 2 AC PSU Bundle	10.10.1000
R9A30A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Back-to-Front 6 Fans 2 AC PSU Bundle	10.10.1000
R8Z96A	Aruba 9300-32D 32-port 100/200/400G QSFP-DD 2-port 10G Switch	10.10.1000

Important information for 9300 Switches

NOTE

Aruba switches covered by this release note use eMMC or SSD storage. This is non-volatile memory for persistent storage of config, files, databases, scripts, and so forth. Aruba recommends updating to version 10.06.0100 or later (including this release) to implement significant improvements to memory usage and prolong the life of the switch.

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

NOTE

Clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes.

To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the `show checkpoint` command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the `Image Version` column in the output of the command, for example CL.10.0*x*.*yyyy*).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.

2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

For information about Short Supported Releases (SSRs) and Long Supported Releases (LSRs), see https://www.arubanetworks.com/support-services/end-of-life/arubaos-software-release/.

To upgrade to:	Your switch must be running this version or later:
AOS-CX 10.12.xxxx Note: 10.12 is an SSR, recommended release is 10.12.0006	AOS-CX 10.09.0002
AOS-CX 10.11.xxxx Note: 10.11 is an SSR, recommended release is 10.11.0001	AOS-CX 10.08.0001

Refer to the Approved Product Lists sites for the Common Criteria, FIPS 140-2 and DoDIN APL to obtain the product certification details. Products should be used as evaluated and defined in the respective configuration guides.

- Common Criteria: https://www.niap-ccevs.org/Product/
- FIPS 140-2: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search
- DoDIN APL: https://aplits.disa.mil/processAPList.action

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open-source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

```
Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
U.S.A.
```

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at: https://hpe.com/software/opensource

Version history

All released versions are fully supported by Aruba, unless noted in the table.

Version number	Release date	Remarks
10.12.1000	02-08-2023	Released, fully supported, and posted on the Web.
10.12.0006	31-05-2023	Released, fully supported, and posted on the Web.

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10 (Version 12 is not supported)

NOTE

Internet Explorer is not supported.

Recommended versions of network management software for switches found in this release note:

Management software	Recommended version(s)
NetEdit	2.8.0
Aruba Central	2.5.7
Central On-Premises	2.5.6.4
Aruba Fabric Composer	6.5.2
Aruba CX Mobile App	Support coming in future release.

NOTE

For more information, see the respective software manuals.

NOTE

To upgrade software using NetEdit, make sure to upgrade to the above version of NetEdit first and then execute the switch software upgrade on devices discovered by this version of NetEdit.

Enhancements

This section describes the enhancements introduced in this release.

Category	Description
Health Monitor	This release introduces new OIDs to the ARUBAWIRED-SYSTEMINFO MIB to enable the reporting of CPU utilization as a one-minute or five-minute average.
Power Management	The ARUBAWIRED-POWERSUPPLY MIB now supports OIDs that report the power supply state as an integer value.
Static VXLAN	Static VXLAN support is introduced in this release.
VXLAN – Multi tenancy	Starting with this release, VLAN translation can be used to achieve Multi tenancy in AOS-CX switches.
VXLAN - IPv6 multicast overlay - Single Fabric	Both IPv6 Multicast routing/bridging over VXLAN overlay within a single fabric is supported.
Multicast ECMP	This release supports Multicast ECMP. Multicast ECMP covers both downstream and upstream ECMP.
VXLAN - IPv6 multicast overlay - Single Fabric	IPv6 Multicast routing over VXLAN overlay with in a single fabric is supported. IPv6 Multicast switching is not supported.
Multicast VXLAN – PIM SSM Overlay	PIM-SSM is supported on a VXLAN overlay. In this release, IPv4 underlay IPv4 overlay with single/multi fabric is supported. IP Multicast Boundary support is not supported in overlay
VXLAN Campus Fabric – Loop prevention	EVPN-VXLAN Campus Fabric should be protected from network loops caused by misconfiguration/miswiring on the edges of the VXLAN fabric. This release enhances the Loop protect feature that prevent loops in VXLAN Fabric.
EVPN-VLAN aware Bundle	The feature introduces support for a VLAN-aware bundle service in accordance with RFC 7432.
VLAN on LLDP advertisements	This feature provides the ability to specify a VLAN instead of the actual IP address for outbound LLDP advertisements. It avoids the need to map port to IP which is error prone. This is newly introduced in AOS-CX and is supported in all platforms except 9300-32C8D.
Hot patch support on 3rd party packages	Hot Patch support is extended for third-party packages, including yocto packages, and security packages.
SSH service ACL	This release introduces the capability to restrict the SSH service with ACLs and object groups, simplifying securing the SSH service
System recovery console	When a system fails to boot to a functional console or repeatedly fails during initialization, the system recovery console with subset of CLI commands tailored for troubleshooting help to restore the system back to a functional state.

Category	Description
	Newly introduced in this releases across all platforms
Deactivate v1 REST API from CX	The REST v1 API are not supported in AOS-CX 10.10 or later releases. However, when users made REST v1 requests, they would get expected responses. As of 10.12, REST v1 will be deactivated, so any REST v1 calls made to the switches will no longer give a 200 or 201 response, and will be forbidden. Network admins that previous used REST v1 calls must update them to use later REST versions.
Unsupported PSU and Fan tray behavior	This change updates unsupported power supply(ies) and/or unsupported fan tray(s) system behavior , and provides clearer fault conditions, error messages, and SNMP traps for to address unsupported power supply(ies) and/or unsupported fan tray(s) condition.

Resolved Issues

This section lists fixes found in this branch of the software. The **Symptom** statement describes what a user might experience if this issue 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 chooses not to update to this version of software.

For a list of issues resolved in the previous releases of 9300 switches, refer to the AOS-CX Release Notes Portal.

NOTE

The Bug ID is used for tracking purposes.

Resolved Issues

This section describes the issues resolved in this release.

Category	Bug ID	Description
BGP	264494	**Symptom**: Routing crashes when adding additional bgp peers to an incomplete peer group configuration. **Scenario**: The hpe-routing process can crash when a second bgp peer gets added to an existing peer group. In this case, the peer group does not have any remote-as associated with it. **Workaround**: Configure the remote-as in the peer group or configure remote-as in all attached peers of the peer group.
Flow Control	258205	**Symptom:** When the switch has a link-level flow-control mode configured on an interface and the link supports auto-negotiation, the flow-control mode used on the local interface is negotiated with the link partner. If the link partner does not negotiate flow-control, no flow-control is applied on the local interface. However, if, for example, the link partner expects to use RXTX link-level flow-control mode but advertises no flow-control mode, the local interface will use no flow-control instead of RXTX link-level flow-control mode. **Scenario:** The link partner should advertise a different flow-control mode than is configured on the local interface on a link that supports auto-negotiation. This will cause the local interface to use negotiated flow-control mode which would be

Category	Bug ID	Description
		different than user configured flow-control mode. **Workaround:** Pauses override functionality to ignore the negotiated flow-control mode on the link and override it with flow-control mode. However, this functionality will only work if the link technology used supports negotiation of flow-control.
Watchdog	258167	**Symptom**: A switch experiences sporadic kernel panic errors. **Scenario**: Switches with exceedingly long cable serial console cables that run in noisy EMI environments can generate random unwanted characters on the serial console line. **Workaround**: Disconnect the long serial console cables when not in use.
VSX	258006	**Symptom**: In a VSX scaled environment, MCLAG links can take more than the intended time to move to forwarding and Up state. **Scenario**: This issue can occur during a VSX Software Upgrade on a VSX scaled environment **Workaround**: Perform a manual upgrade in a scaled VSX environment, bu upgrading the VSX-Secondary first followed by the VSX-Primary
CLI	257999	**Symptom**: A ten to twelve second delay in the initial output for the **show mac-address-table** command causes some internal scripts to time out. **Scenario**: This issue can occur in deployments with a large MAC scale (greater than 8k entries).
SNMP	257729	**Symptom:** Incorrect BGP remote peer IP information is sent via SNMP. **Scenario:** In deployments with a BGP peer-group configuration, an SNMP walk for bgpPeerRemoteAddr (id 1.3.6.1.2.1.15.3.1.7) displays a random IP address in the output.
SNMP	257161	**Symptom:** Incorrect responses are return from SNMP when **IF-MIB:ipNetToPhysicalTable** (1.3.6.1.2.1.4.35) is walked **Scenario:** This issue occurs while performing an snmpwalk on 1.3.6.1.2.1.4.35, which will return an index value of '**0**' for every response.
REST	256915	**Symptom:** TACACS+ Authorization packets are sent with empty values in the remote address field for REST-API based user sessions, causing the firmware upgrade to fail. **Scenario:** When using the REST API on the switch with TACACS+ Authorization configured, the switch will send a request packet with an empty value for the remote address field. Some TACACS+ servers require the remote address field to contain a unique value to identify the network device.
TACACS	256739	**Symptom:** A user login or command authorization causes **systemd-coredump – vtysh** to crash due to signal 6. **Scenario:** The ciphertext TACACS key is extracted from the active configuration and converted internally to plaintext for use with communication with the TACACS server. A buffer overflow will occur if the decrypted plaintext key from the cipher text is more than 32 bytes. **Workaround:** Reconfigure TACACS server with a plaintext key

Category	Bug ID	Description
		fewer than 32 bytes.
VRF	253907	**Symptom:** When a static IVRL route with a nexthop-interface (as opposed to a nexthop IP address) is used to leak a default route, it causes performance issues as the packets will be CPU forwarded. **Scenario:** If, for example, a source VRF prefix 10.0.0.0/8 is configured in interface 1/1/1 (belonging to the source VRF), it can be leaked to destination VRF with static IVRL configuration as **ip route 10.0.0.0/8 1/1/1 vrf destination**. Static IVRL with nexthop as interface should be used to leak prefixes that are only directly accessible from source VRF. Otherwise ARP entries with respect to nexthop will not be leaked to destination VRF. **Workaround:** Use dynamic route leaking using BGP between source and destination VRFs. Static IVRL should not be used to leak default Route with nexthop interface only, or any prefixes which are not directly connected to the source VRF
Ping	253583	**Symptom:** A ping with an MTU of 9170 or greater fails ISL. **Scenario**: This behavior is specific to ping packets. It is not affecting any other types of traffic with large MTU.
L3 Addressing	253444	**Symptom:** Users are unable to configure a reserved IPv6 anycast address under an interface. **Scenario:** This issue occurs when configuring an IPv6 address with the interface identification field **ffff**.
Certificate Manager	252882	**Symptom:** Certificate verification on the switch for a service or client trying to connect to the switch may fail at the OCSP verification stage for some PKI configurations. **Scenario:** This issue can occur if the peer certificate representing the remote server or client has an OCSP URL embedded, and if its OCSP signer CA certificate is an intermediate certificate and installed as a TA profile in the switch before its root CA and other higher CAs in the certificate chain.
OSPFv2	252504	**Symptom:** The best path selection is inaccurate when a switch receives the same network from two different OSPF processes within the same VRF. **Scenario:** Redistribute the same network under two different OSPF processes in the network. When the switch receives this same network from two different processes, it ignores the "cost" in best path selection and results in an incorrect route installed in the routing table.
BGP	251309	**Symptom:** Aggregate routes are not advertised to the peer when the aggregator learns the same prefix from the peer. **Scenario:** This issue occurs when configuring two BGP peers, when there are aggregate routes on one of the peers and the other peer sends back a route which is part of the aggregated route. **Workaround:** Use network configuration to statically aggregate the routes.
BGP	245472	**Symptom:** When BGP neighbors an of L2VPN EVPN family are changed from dynamic BGP peering to static BGP peering

Category	Bug ID	Description
		using checkpoint, the sessions get stuck in Idle state. **Scenario:** This issue occurs when static BGP L2VPN EVPN peers are configured and saved as checkpoint, and that is removed and Dynamic BGP L2VPN EVPN peering is configured. When static BGP L2VPN EVPN peering is brought back using first checkpoint, the session is seen to be stuck in idle state. **Workaround:** Remove and re-add the configuration manually.
BGP	242032	**Symptom**: The BGP peer cannot ping the loopback configured in VRF-A although looback route is leaked into VRF-B from VRF-A. **Scenario**: This issue can occur when VRFs are both configured for dynamic Route Leaking, th switch has an iBGP peering in VRF-B, nd loopbacks are redistributed using BGP from VRF-A to VRF-B. Although Routing tables look fine on both VRFs, the Loopback is NOT advertised by the egress VRF-A.
OSPFv2	234516	**Symptom:** An OSPF router takes one extra hop to reach the external network. **Scenario:** When OSPF imports a static route, and the next hop link is OSPF enabled, all other routers in the area send traffic to ASBR instead of the shortest NH router path.
DNS	230380	**Symptom:** The switch experiences high CPU utilization. **Scenario:** High CPU utilization is observed when SNMP invokes DNS resolution. It is due to access of source IP which causes CPU overhead.

Feature Caveats

The following are feature caveats that should be taken into consideration when using this version of the software.

Feature	Description
REST	The REST v1 API that was deprecated in previous release of AOS-CX is completely deactivated and no longer available in AOS-CX 10.12. For more information on migrating your deployment from the RESTv1API to the RESTv10.xx API, refer to the REST API Migration Quick Start Guide.
PIM-SM	Pim Active-Active is not supported on overlay VXLAN SVIs.
SNMP	When SNMP is enabled via the switch CLI, it can take between 1-2 minutes for the SNMP daemon to be ready to respond to requests. If a local or external SNMP MIB walk is performed in the interval between when SNMP is first enabled and the SNMP daemon is ready, the MIB walk action will return an error.
Certificates	When a switch uses a certificate with a legacy certificate name that is not supported in 10.12 because it contains disallowed characters, the information will migrate properly in the upgrade, but that certificate can no longer be edited. For new certificate names, only alphanumeric characters, dots, dashes, and underscores are allowed.

Feature	Description
Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
IGMP/PIM on 6-in-6, Loopback and GRE interfaces	IGMP cannot be enabled on either Loopback or GRE interfaces. IGMP and PIM is not supported on a 6-in-6 Tunnel.
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
PFC	Priority-based flow control (PFC) is not supported on a split port.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.

Known Issues

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.

Category	Bug ID	Description

Upgrade information

AOS-CX 10.12.0006 uses ServiceOS CL.01.12.0002.

Each VSX switch in a pair must run the same version of AOS-CX. If a primary VSX switch is upgraded to 10.10.xxxx, the secondary VSX switch must be immediately upgraded to that same version. If the ISL link is disabled and enabled on VSX switches that are running different versions of AOS-CX, a VSX secondary switch running an older version of AOS-CX may be unable to synch information from the VSX primary, which can cause the port state to become blocked and lead to traffic loss.

Do not interrupt power to the switch during this important update.

Manual configuration restore for software downgrade

To restore a previous configuration when downgrading to a previous version of software, follow these steps:

1. Use the **show checkpoint** command to see the saved checkpoints and ensure that you have a checkpoint that is an exact match of the target software version (see the **Image Version** column in the output of the command, for example, CL.10.xx.*yyyy*).

   This checkpoint can be the startup-config-backup automatically created during the initial upgrade or any other manually created checkpoint for the target software version.
2. Copy the backup checkpoint into the startup-config.
3. Boot the switch to the target version (lower version), making sure to select `no` when prompted to save the current configuration.

Performing the upgrade

For additional upgrade and downgrade scenarios, including limitations of automatic upgrade and downgrade scenarios provided by the Configuration Migration Framework (CMF), refer to the **AOS-CX 10.12 Fundamentals Guide**.

This version may contain a change of BootROM from the current running version. A BootROM update is a non-failsafe update. Do not interrupt power to the switch during the update process or the update could permanently damage the device.

1. Copy the new image into the non-current boot bank on the switch using your preferred method.
2. Depending on the version being updated, there may be device component updates needed. Preview any devices updates needed using the `boot system <BOOT-BANK>` command and entering `n` when asked to continue.

   For example, if you copied the new image to the secondary boot bank and no device component updates are needed, you will see this:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
```

   In this example, three device updates will be made upon reboot, one of which is a non-failsafe device:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

2 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
```

```
There may be multiple reboots during the update process.

1 non-failsafe device(s) also need to be updated.
Please run the 'allow-unsafe-updates' command to enable these updates.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
```

3. When ready to update the system, if a non-failsafe device update is needed, make sure the system will not have any power interruption during the process. Invoke the `allow unsafe updates` command to allow updates to proceed after a switch reboot. Proceed to step 4 within the configured time.

```
switch# config
switch(config)# allow-unsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin
applying any needed updates.  Ensure that the switch will not lose power,
be rebooted again, or have any modules removed until all updates have
finished and all line and fabric modules have returned to the ready state.

WARNING: Interrupting these updates may make the product unusable!

Continue (y/n)? y

    Unsafe updates      : allowed (less than 30 minute(s) remaining)
```

4. Use the `boot system <BOOT-BANK>` command to initiate the upgrade. On the switch console port an output similar to the following will be displayed as various components are being updated:

```
switch# boot system secondary
Default boot image set to secondary.
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...
Done checking for updates.

3 device(s) need to be updated during the boot process.
The estimated update time is between 2 and 3 minute(s).
There may be multiple reboots during the update process.


This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

Looking for SVOS.

Primary SVOS:  Checking...Loading...Finding...Verifying...Booting...

ServiceOS Information:
```

```
    Version:          <serviceOS_number>
    Build Date:       yyyy-mm-dd hh:mm:ss PDT
    Build ID:         ServiceOS:<serviceOS_number>:6303a2a501ba:202006171659
    SHA:              6303a2a501bad91100d9e71780813c59f19c12fe

Boot Profiles:

0. Service OS Console
1. Primary Software Image [xx.10.11.1010]
2. Secondary Software Image [xx.10.12.1000]

Select profile(secondary):

ISP configuration:
    Auto updates        : enabled
    Version comparisons : match (upgrade or downgrade)
    Unsafe updates      : allowed (less than 29 minute(s) remaining)

Advanced:
    Config path         : /fs/nos/isp/config [DEFAULT]
    Log-file path       : /fs/logs/isp [DEFAULT]
    Write-protection    : disabled [DEFAULT]
    Package selection   : 0 [DEFAULT]

3 device(s) need to be updated by the ServiceOS during the boot process.
The estimated update time by the ServiceOS is 2 minute(s).
There may be multiple reboots during the update process.


MODULE 'mc' DEVICE 'svos_primary' :
    Current version  : '<serviceOS_number>'
    Write-protected  : NO
    Packaged version : '<version>'
    Package name     : '<svos_package_name>'
    Image filename   : '<filename>.svos'
    Image timestamp  : 'Day Mon dd hh:mm:ss yyyy'
    Image size       : 22248723
    Version upgrade needed

Starting update...

Writing...    Done.
Erasing...    Done.
Reading...    Done.
Verifying...  Done.
Reading...    Done.
Verifying...  Done.


Update successful (0.5 seconds).

reboot: Restarting system
```

Multiple components may be updated and several reboots will be triggered during these updates. When all component updates are completed, the switch console port will arrive at the login prompt with a display similar to following:

```
(C) Copyright 2017-2023 Hewlett Packard Enterprise Development LP

                    RESTRICTED RIGHTS LEGEND
```

```
 Confidential computer software. Valid license from Hewlett Packard Enterprise
 Development LP required for possession, use or copying. Consistent with FAR
 12.211 and 12.212, Commercial Computer Software, Computer Software
 Documentation, and Technical Data for Commercial Items are licensed to the
 U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com

switch login:
```

Aruba recommends waiting until all upgrades have completed before making any configuration changes.

Chapter 2
Other resources

Aruba is committed to ensuring you have the resources you need to be successful. Check out these learning and documentation resources:

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX 10.11 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

Chapter 3
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/. 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.