Copyright Information
© Copyright 2022 Hewlett Packard Enterprise Development LP.

Open Source Code
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
6280 America Center Drive
San Jose, CA 95002
USA

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.


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.
Description
This release note covers software versions for the AOS-CX 10.08 branch of the software.

If you run the `show version` command on the switch, the version number will display TL.10.08.xxxx, where xxxx is the minor version number.

AOS-CX is a new, modern, fully programmable operating system built using a database-centric design that ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including the features included in the Enhancements section of this release note. Version 10.08.0001 is the initial build of major version 10.08 software.

Products supported
This release applies to the 8320 Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

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

<table>
<thead>
<tr>
<th>Product number</th>
<th>Product name</th>
<th>Minimum software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>JL579A</td>
<td>Aruba 8320 32p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
<td>10.00.0008</td>
</tr>
<tr>
<td>JL581A</td>
<td>Aruba 8320 48p 1G/10GBASE-T and 6p 40G QSFP+ with X472 5 Fans 2 Power Supply Switch Bundle</td>
<td>10.00.0013</td>
</tr>
</tbody>
</table>

Important information for 8320 Switches
To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Diffie-Helman algorithm is no longer enabled by default for key exchange. To enable using Diffie-Helman for key exchange, use the command `ssh key-exchange-algorithms <KEY-EXCHANGE-ALGORITHM-LIST>`.
In this and previous releases, AOS-CX BGP implementations support resolving a BGP route's nexthop to a default route (0.0.0.0/0). However, this is not generally recommended in network deployments. Considering the default route to be the last resort route, resolving the BGP route's nexthop to a default route can cause potential routing loops in the network, if they are not properly designed and monitored. Route flaps and/or traffic drops may be observed in such cases.

In a future release, AOS-CX will not support the BGP route's nexthop resolving to a default route in the Route table. To avoid this problem and to be prepared for the update, Aruba recommends configuring a more specific static route (or host route) for BGP nexthops that are multihops away that are resolving via the default route.

If using the Web UI, you should 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.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00xx version of software to 10.09.xxxx.

To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where `<VLAN_ID>` is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

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, TL.10.0x.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.

**Industry and government certifications**

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

**License written offer**

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](https://hpe.com/software/opensource)

**Version history**

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

<table>
<thead>
<tr>
<th>Version number</th>
<th>Release date</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08.1060</td>
<td>2022-05-02</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1050</td>
<td>2022-03-15</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1040</td>
<td>2022-01-31</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1030</td>
<td>2021-12-09</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1023</td>
<td>2021-12-17</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1021</td>
<td>2021-11-08</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.1010</td>
<td>2021-09-21</td>
<td>Released, fully supported, and posted on the web.</td>
</tr>
<tr>
<td>10.08.0001</td>
<td>2021-08-13</td>
<td>Initial release of AOS-CX 10.08. Released, fully supported, and posted on the web.</td>
</tr>
</tbody>
</table>

**Compatibility/interoperability**

The switch web agent supports the following web browsers:
### Browser Minimum supported versions

<table>
<thead>
<tr>
<th>Browser</th>
<th>Minimum supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge (Windows)</td>
<td>41</td>
</tr>
<tr>
<td>Chrome (Ubuntu)</td>
<td>76 (desktop)</td>
</tr>
<tr>
<td>Firefox (Ubuntu)</td>
<td>56</td>
</tr>
<tr>
<td>Safari (MacOS)</td>
<td>12</td>
</tr>
<tr>
<td>Safari (iOS)</td>
<td>10 (Version 12 is not supported)</td>
</tr>
</tbody>
</table>

Internet Explorer is not supported.

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

<table>
<thead>
<tr>
<th>Management software</th>
<th>Recommended version(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airwave</td>
<td>8.2.14.0</td>
</tr>
<tr>
<td>NetEdit</td>
<td>2.4.0</td>
</tr>
<tr>
<td>Aruba CX Mobile App</td>
<td>2.7.9 (or later)</td>
</tr>
<tr>
<td>Aruba Central</td>
<td>2.5.4</td>
</tr>
<tr>
<td>Network Automation</td>
<td>10.10, 10.11, 10.20, 10.21, 10.30, 10.40</td>
</tr>
<tr>
<td>Network Node Manager</td>
<td>10.10, 10.20, 10.21, 10.30, 10.40</td>
</tr>
<tr>
<td>IMC</td>
<td>7.3 (E0706)</td>
</tr>
</tbody>
</table>

For more information, see the respective software manuals.

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 lists enhancements added to this branch of the software.

The number listed with the category is used for tracking purposes.

**Enhancements for 8320 Switches in AOS-CX 10.08.1060**

There are no new enhancements in this release.

**Enhancements for 8320 Switches in AOS-CX 10.08.1050**

No enhancements were included in version 10.08.1050.
Enhancements for 8320 Switches in AOS-CX 10.08.1040
No enhancements were included in version 10.08.1040.

Enhancements for 8320 Switches in AOS-CX 10.08.1030
No enhancements were included in version 10.08.1030.

Enhancements for 8320 Switches in AOS-CX 10.08.0021
This section lists enhancements added to this branch of the software.

The number listed with the category is used for tracking purposes.

The following enhancements were introduced in AOS-CX 10.08.0021

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Added next-server support for BOOTP options in DHCP server for the client's</td>
</tr>
<tr>
<td>187222</td>
<td>bootstrap process. This option can be added to the DHCP server option</td>
</tr>
<tr>
<td></td>
<td>configuration using the next-server command.</td>
</tr>
<tr>
<td></td>
<td>See Documentation Updates and Corrections for more information.</td>
</tr>
<tr>
<td>SNMP</td>
<td>The hpSwitchPortFdbVidList MIB OID has been added to display port VLAN</td>
</tr>
<tr>
<td>195627</td>
<td>membership.</td>
</tr>
</tbody>
</table>

Enhancements for 8320 Switches in AOS-CX 10.08.1010
This section lists enhancements added to this branch of the software.

The number listed with the category is used for tracking purposes.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics</td>
<td>AIOPS - NAE Agent and Engine improvements for unicast routing.</td>
</tr>
<tr>
<td></td>
<td>AIOPS - NAE Agent and Engine improvements for client services.</td>
</tr>
</tbody>
</table>

Enhancements for 8320 Switches in AOS-CX 10.08.0001
This section lists enhancements added to this branch of the software.

The number listed with the category is used for tracking purposes.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>BGP fast-external-failover is now enabled by default.</td>
</tr>
<tr>
<td>DHCP relay</td>
<td>Added DHCP relay coexistence with DHCP server for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>Inclusive terminology</td>
<td>As part of advancing HPE's and Aruba's commitment to racial justice, we are</td>
</tr>
<tr>
<td></td>
<td>taking a much-needed step in overhauling engineering terminology to reflect</td>
</tr>
<tr>
<td></td>
<td>our belief system of diversity and inclusion. See</td>
</tr>
</tbody>
</table>
### Category Description

- **Job Scheduler**: Added the ability to execute required CLI commands at a specific time and date. This can be repeated at periodic intervals.
- **Loopback IP redistribution in OSPF**: Allows redistribution of IPv4 and IPv6 addresses of loopback interfaces in OSPFv2 and OSPFv3.
- **MAC Tables 74408**: Added an SNMP trap notification if there is a MAC address change.
- **MAC Tables 84378**: Added the `clear mac` command to delete a specific MAC on one or more VLANs.
- **Network Load Balancing (NLB)**: Provides load balancing technology for server clustering developed on Microsoft Windows Server. Supports load sharing and redundancy among servers within a cluster.
- **Security**: Ensures configuration integrity. Limit concurrent users for web access.
- **Transceivers 160269**: Added display in dBm for DOM thresholds in the output of the `show interface dom detail` command.
- **VSX 162842**: Updated the warning message displayed when shutting down an Switch Virtual Interface (SVI) with an active gateway enabled to be more informative about the risks of doing such a shutdown.

### Resolved Issues
This section lists released builds that include fixes found in this branch of the software. 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 **Bug ID** is used for tracking purposes.

#### Resolved issues for 8320 Switches in Version 10.08.1060

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| sFlow          | 222039     | **Symptom**: The switch will stop responding with logs indicating the ops-switchd process  
|                | 221443     | **Scenario**: This issue can occur when configuring sFlow on the switch with multiple LAGs on the system.  
<p>|                |            | <strong>Workaround</strong>: Disable sFlow on the switch.                                   |
| Multicast      | 220354     | <strong>Symptom</strong>: While the IGMP static group is configured in the interface     |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| Symptom           | 219328    | **Symptom:** The `snmp-server snmpv3 only` CLI command incorrectly allows an SNMP v1/v2 walk, though an SNMPv2 walk with the community (which is mapped to context) works as expected. **Scenario:** Configure this feature using the command `snmp-server snmpv3-only` and `snmpv3 context <context-name> vrf <vrf-name> community <community-name>`.

| SNMP              | 215672    | **Symptom:** GET requests made to LAG interfaces collection through REST API do not include the `type` field. **Scenario:** GET `/rest/v10.04/system/interfaces/lag<ID>` response does not include the `type` field. **Workarounds:** Add category": "status" to the `type` column in the Port table. |

| CHEOPS            | 211222    | **Symptom:** Link status traps are not sent when using minimal SNMP config. **Scenario:** When SNMP is globally enabled, it is expected that link status traps are sent by default when a physical port link state transitions. A change was introduced in ArubaOS-CX to include IF-MIB link status traps, but were disabled by default. The traps will not be sent unless explicitly enabled using the `trap link-status` command under the interface configuration context. **Workaround:** Manually enable traps on a per-interface basis using `trap link-status`. |

| Physical Interfaces | 219131    | **Symptom:** After uploading switch firmware using the web interface, the user is logged out. **Scenario:** This issue occurs when the filename of the new firmware contains a special character like `()`&`#`. **Workarounds:** Ensure the firmware file name being uploaded has only alphanumeric characters and the allowed special characters period (.), underscore (_), and dash (-). |

| WebUI             | 209933    | **Symptom:** After an unspecified period of time the DHCP Server service stops leasing ip addresses to clients. **Scenario:** The DHCP server service writes to a temporary log file that can grow without bounds over time until the point that the filesystem is full and service is stopped. **Workarounds:** Rebooting the switch will temporarily clear the log file and free the filesystem. |

<p>| ARP Security      | 217116    | <strong>Symptom:</strong> Ping to neighbor is fails and the ARP address is not learned. <strong>Scenario:</strong> ARP address is not learned when ARP Inspection with DHCP Snooping is enabled on a VLAN and the VLAN interface obtains an IP address via the <code>ip dhcp</code> command. <strong>Workarounds:</strong> Ensure the VLAN interface is getting an IP address. |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| Boot Process  | 216818  | **Symptom:** The output of the `show boot-history` command displays an incorrect uptime.  
**Scenario:** This issue can occur in a deployment with NTP and Aruba Central enabled, if the switch fails to connect with Aruba Central and continues to retry.  
**Workaround:** The customer can disable Aruba Central using the following CLI command.  
`switch (config)# aruba-central`  
`switch (config-aruba-central)# disable` |
| CHEOPS        | 215672  | **Symptom:** GET requests made to LAG interfaces collection through REST API do not include the `type` field.  
**Scenario:** GET `/rest/v10.04/system/interfaces/lag<ID>` response does not include the `type` field.  
**Workaround:** Add category”: “status” to the `type` column in the Port table. |
| OSPFv2        | 209332  | **Symptom:** OSPF routes are not redistributed when a route-map with deny tag is applied.  
**Scenario:** Once the tag value is set to an OSPF route using route-maps, the tag is not reset even when the route is updated from a route-source without any tag.  
**Workaround:** Disable and enable OSPF on all the switches which has this learnt route. |
| DHCP Server   | 209933  | **Symptom:** After an unspecified period of time the DHCP Server service stops leasing IP addresses to clients.  
**Scenario:** The DHCP server service writes to a temporary log file that can grow without bounds over time until the point that the filesystem is full and service is stopped.  
**Workaround:** Rebooting the switch will temporarily clear the log file and free the filesystem. |

**Resolved issues for 8320 Switches in Version 10.08.1050**

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| ASIC SDK      | 211181  | **Symptom:** The switch can stop responding on rare instances of ASIC memory error correction.  
**Scenario:** This issue can occur during normal usage. |
| RADsec        | 211033  | **Symptom:** Management RADIUS accounting packets are not sent via RADSEC connection.  
**Scenario:** When remote accounting is enabled, all accounting packets will be sent to the RADIUS server. When a RADSEC server is configured as a remote server for accounting, accounting packets are not being sent to server. |
| MAC tables    | 202739  | **Symptom:** Network traffic appears to cease for up to 5 minutes.  
**Scenario:** When a Topology Network Change (TCN) event affects a large number of MAC addresses, typically across multiple ports, the internal MAC cache can become temporarily out of sync with OVSDB. This situation is corrected after a 5 minute "retry" timing expires.  
**Workaround:** Prevent TCN events from reaching core systems with appropriate STP configuration (TCN guard). The system will correct itself after the retry timer expires.  
|               | 195310  |                                                                                                                                          |
|               | 192968  |                                                                                                                                          |
## Resolved issues for 8320 Switches in Version 10.08.1040

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| MSTP           | 209003  | **Symptom:** Performing an SNMP walk for spanning-tree MIBs can cause the SNMP daemon to stop responding.  
**Scenario:** This issue can occur when an SNMP walk is performed during initial setup of a VSF stack, when STP is not fully converged.  
**Workaround:** Avoid performing an SNMP walk during initial setup of the VSF stack. |
| MDNS-SD        | 206140  | **Symptom:** The switch is running out memory, leading to kernel crash for the mDNS daemon.  
**Scenario:** This issue is caused by a memory issue in the `svcdisc-qwd` daemon with mDNS query response packets.  
**Workaround:** Restart the `svcdisc-qwd` daemon after the switch consumes 1Gb of memory. |
| ARP            | 205621  | **Symptom:** Neighbors are learned from GRAT ARP (ARP announcement) from an unmatched subnet.  
**Scenario:** When GRAT ARP is received on a port with ARP suppression enabled and the target IP does not match the subnet of the port, the device still learns the neighbor.  
**Workaround:** Disable processing of GRAT ARP using the `no arp process-grat-arp` command. |
| VSF            | 208611  | **Symptom:** 6200/6300 Series switches in a VSF stack cannot be provisioned using Aruba Central.  
**Scenario:** When a VSF stack is upgraded from a release earlier than AOS-CX 10.07.0001 to a release later than 10.07.0001, the conductor of the stack should be elected as a non-primary device (that is, not member1). However, an issue occurs where the stack_id is not populated in database to which Central subscribes preventing the switches in the stack from being onboarded to Central.  
**Workaround:** Reboot the stack system experiencing this issue. After the system reboots, member-1 becomes the conductor, and the issue resolves. |
| MSTP           | 207537  | **Symptom:** An intermittent timing issue occurs when port forwarding state changes. The link up but no traffic passes while connecting new devices on switch port.  
**Scenario:** This issue occurs when the port forwarding state and STP enablement changes.  
**Workaround:** Disable and then re-enable the port or STP to resolve this issue. |
| VRRP           | 203303  | **Symptom:** Frequent VRRP interface flaps resulted in user outages across VLANs.  
**Scenario:** VRRP flaps and excessive packet drops are observed between a pair of switches when the VRRP advertisement interval timer is set to 1 second and SNMP inform is enabled.  
**Workaround:** Increase the VRRP advertisement interval time to 3 seconds. |
| Config Mgmt    | 202629  | **Symptom:** A running configuration is not copied to an external storage server.  
**Scenario:** The `copy running-configuration` command fails to copy a configuration to an external storage server using SFTP, TFTP or SCP protocols. |
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| Config Mgmt | 209025 | **Symptom:** The write memory and copy running-config commands fail to save the running configuration, and the operation fails after five minutes.  
**Scenario:** When running the write memory or copy running-config commands on an 8325 switch in a VSX stack, the commands fail to save the configuration, and the output of the command displays the warning **timeout due to waiting for database processing permission took more than 300 seconds.**  
**Workaround:** Restart the RESTd daemon or reboot the switch. |
| BGP         | 208535 | **Symptom:** When IPv6 address of a loopback interface is changed, all the BGP sessions that are formed by using the IP of that loopback interface are restarted.  
**Scenario:** The expected behavior is that when the IPv6 address of a loopback interface is changed, only the BGP sessions that are formed using the IPv6 address of that loopback interface are restarted. The switch incorrectly allows IPv4 BGP sessions to restart when the IPv6 address of a loopback interface is changed. |
| ACL         | 207037 | **Symptom:** Access control list (ACL) ranges do not match appropriate traffic. The access list entry (ACE) behaves as if it has no source or destination port ranges.  
**Scenario:** The range checker used in the ACL is not matching DNS traffic and blocks access to Web sites.  
**Workaround:** The workaround is to use the eq operator and individual ports instead of port ranges. This can be resolved by calling the function that qualifies on the range during the entry installation. |
| BGP         | 205775 | **Symptom:** A switch does not return BGP Neighbor statistics when GET requests for the BGP Neighbor table were called via the REST API.  
**Scenario:** This issue occurred when there were neighbor statistics for BGP sessions between multiple different deployment sites.  
**Workaround:** View statistics using the command-line interface. CLI statistics are correct during the same time. |
| System      | 203083 | **Symptom:** A Kernel panic error occurs on the switch due to a machine check exception.  
**Scenario:** This issue is not impacted by the switch configuration. |

**Resolved issues for 8320 Switches in Version 10.08.1030**

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| ARP      | 205621 | **Symptom:** Neighbors are learned from GRAT ARP (ARP announcement) from an unmatched subnet.  
**Scenario:** When GRAT ARP is received on a port with ARP suppression enabled and the target IP does not match the subnet of the port, the device still learns the neighbor.  
**Workaround:** Disable processing of GRAT ARP using the no arp process-grat-arp command. |
| BGP      | 203620 | **Symptom:** The switch experiences an hpe-routing crash.  
**Scenario:** In rare instances, when the aggregate address config is removed or changed to aggregate address summary-only, the switch experiences an hpe-routing crash. |
### Symptom:
The switch loses access to Central.
### Scenario:
Access to Central can be lost in any of the following three scenarios:
- When a config has been pushed from Central and an attempt to overwrite the config with a new template containing the same DNS config.
- When the same static DNS is configured and then Central pushes a template to the switch through VLAN 1.
- When pushing a DNS config through Central if there is a DHCP update on VLAN 1 from the firewall, the resolv.conf file is overwritten with a new IP address.
### Workaround:
Remove the static DNS configuration and add it back.

### Symptom:
MAC addresses are not learned for clients on non-ERPS ring ports causing client traffic to be dropped.
### Scenario:
When spanning tree is disabled on the switch and ERPS is enabled, MAC addresses do not get learned for clients on non-ERPS ring ports, causing the traffic from those clients to be dropped.
### Workaround:
Enable spanning tree on the switch.

---

### Resolved issues for 8320 Switches in Version 10.08.1021

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 Routes</td>
<td>195719</td>
<td><strong>Symptom:</strong> Static and dynamic routes are not installed. <strong>Scenario:</strong> After a switch boot or switchover, when using the <code>show ip route</code> or <code>show ipv6 route</code> commands, no dynamic or static routes are displayed. <strong>Workaround:</strong> Reboot the switch.</td>
</tr>
<tr>
<td>L3 Routes</td>
<td>197292</td>
<td><strong>Symptom:</strong> Route 128.0.0.0/1 is not installed in the routing table. <strong>Scenario:</strong> If BGP/OSPF has learned the route 128.0.0.0/1 from its peer, it will be present in the BGP/OSPF table but is not installed into the routing table RIB (<strong>show ip route</strong>).</td>
</tr>
</tbody>
</table>
| Link Aggregation | 194007  | **Symptom:** The LAG interface is stuck in LACP-block. **Scenario:** When the startup config has a LAG interface configured and the configuration is loaded using the management port, LAG creation fails and a message similar to the following is seen in `/var/log/messages`:

- 2021-08-16T02:11:20.900439+00:00 6300 ip[4566]: 2021-08-16T02:11:20Z|00003|portd_linux_bond|ERR|bond: Failed to create bond lag1 in linux table 0
- 2021-08-16T02:11:20.900490+00:00 6300 ip[4566]: 2021-08-16T02:11:20Z|00004|portd_tx|ERR|LAG bond lag1 - netdev creation failed in vrf table 0
**Workaround:** Reboot the switch. |
<p>| Logging        | 195946  | <strong>Symptom:</strong> An error message is logged that says the cron daemon was unable to move a log file because the name is too long. <strong>Scenario:</strong> When the switch hostname contains non-numeric characters, the logrotate feature incorrectly renames the file, causing an error message because the name is too long. |
| OSPF           | 194375  | <strong>Symptom:</strong> A UBT client is unable to get a DHCP IP address post- |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>authorization or the switch experiences a total traffic loss for already-authorized and working UBT clients.</strong> <strong>Scenario:</strong> When a two-member VSF access switch is connected to a VSX core switch with two ROP uplinks (ECMP) to each VSX core switch and OSPF is enabled on both uplinks, if one of the uplinks is flapped from the VSF switch or both uplinks are flapped one after the other in quick succession (less than 30 seconds) or one of the VSX core switches is rebooted, UBT clients are unable to get a DHCP address or the switch experiences a total loss of traffic for already-authorized UBT clients. <strong>Workaround:</strong> Any of these three workarounds can be used: Delete and add the impacted UBT zone configuration. Reboot the VSF switch stack. Configure OSPF interface cost on the VSF switch stack.</td>
</tr>
<tr>
<td>PBR</td>
<td>196525</td>
<td><strong>Symptom:</strong> The switch crashes and a core dump is generated. <strong>Scenario:</strong> Under certain conditions, when a PBR policy is applied to an SVI and checkpoints are saved and restored, a crash occurs and a core dump is generated. <strong>Workaround:</strong> Reboot the switch.</td>
</tr>
<tr>
<td>REST</td>
<td>200118</td>
<td><strong>Symptom:</strong> User authentication in the Web UI fails. <strong>Scenario:</strong> When using RADSEC as the authentication server, attempts to authenticate in the Web UI fail.</td>
</tr>
<tr>
<td>SNMP</td>
<td>195302</td>
<td><strong>Symptom:</strong> When queried for sysObjectID.0, the switch returns an error, no such object. <strong>Scenario:</strong> During a boot of the switch, if AOS-CX is still loading and a query is made for sysObjectID.0, the switch will return an error that the object does not exist. <strong>Workaround:</strong> Wait a few moments for the switch to complete booting and perform the query again.</td>
</tr>
<tr>
<td>VSX Sync</td>
<td>196010</td>
<td><strong>Symptom:</strong> DHCP server configurations between VSX pairs do not match. <strong>Scenario:</strong> In a VSX topology using vsx-sync dhcp-server in the VSX context, the DHCP server configuration fails to copy to the secondary switch. <strong>Workaround:</strong> Turn off the DHCP server configuration sync in the vsx context and perform a manual configuration on the secondary switch.</td>
</tr>
<tr>
<td>VSX Sync</td>
<td>201013</td>
<td><strong>Symptom:</strong> The config changes made to the primary switch stop syncing to the secondary switch. <strong>Scenario:</strong> With a large config, after a long time without changes to the config, the vsx-syncd daemon becomes unresponsive and changes to the primary are not synced to the secondary. <strong>Workaround:</strong> Restart the vsx-syncd daemon.</td>
</tr>
<tr>
<td>VXLAN</td>
<td>188001</td>
<td><strong>Symptom:</strong> The switch fails to import the routing table (RT) for some VRFs. <strong>Scenario:</strong> When a VRF is named with the keyword mgmt in the name (for example, testmgmt or mgmt-aps), the switch fails to import the RT to the EVPN table. <strong>Workaround:</strong> Rename the VRF to remove the mgmt keyword.</td>
</tr>
</tbody>
</table>

**Resolved issues for 8320 Switches in Version 10.08.1010**
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| ACLs       | 193057  | **Symptom:** The switch crashes when a VLAN ACL is configured using REST.  
**Scenario:** When REST is used to configure a VLAN ACL using `in` rather than `routed-in`, the switch crashes.                              |
| Logging    | 195946  | **Symptom:** An error message is logged that says the cron daemon was unable to move a log file because the name is too long.  
**Scenario:** When the switch hostname contains non-numeric characters, the logrotate feature incorrectly renames the file, causing an error message because the name is too long. |
| PIM-SM     | 190657  | **Symptom/Scenario:** The switch does not elect the correct BSR after changing the BSR priority or changing to auto RP from static RP.  
**Workaround:** Configure the candidate BSR on only one node of the VSX environment or toggle the router PIM status using the `router pim disable` and `router pim enable` commands. This is resolved in AOS-CX 10.07.0030 or later releases. |
| SNMP       | 189372  | **Symptom:** `dot1dStpPortPathCost` reflects the open-path-cost and does not match the CLI.  
**Scenario:** When using SNMP to identify spanning tree state and values, `dot1dStpPortPathCost` does not report the value it should.  
**Workaround:** Use the `show spanning-tree` command to view the correct values. |
| TACACS     | 194803  | **Symptom:** The user is authenticated as local rather than remote (TACACS).  
**Scenario:** When the TACACS server is configured with FQDN and TACACS authentication is configured, the user is authenticated with local credentials instead of with remote TACACS authentication.  
**Workaround:** Configure the TACACS server with an IP address rather than FQDN. |
| VRRP       | 189958  | **Symptom:** The VRRP high priority master ignores the configured Preempt Delay Timer (PDT) and assumes the Master role only after the Master Down Timer (MDT) expiry after reboot.  
**Scenario:** When the PDT is configured with a higher value than the MDT, the PDT is ignored by the VRRP high priority master which waits for the PDT to expire before going to Master after a reboot.  
**Workaround:** Configure the MDT to be greater than or equal to the PDT. |
| VSX Sync   | 193962  | **Symptom:** VSX sync stops working. Logs still show activity in the secondary VSX sync, but no updates are received from the primary switch.  
**Scenario:** In a VSX topology when both switches become disconnected (for example, through an ISL disconnect or a failover) for an extended period of time, VSX sync stops working when the switches come back online.  
**Workaround:** On the secondary switch, restart VSX sync using the `systemctl restart vsx-syncd` command. |

Resolved issues for 8320 Switches in Version 10.08.0001
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| ARP               | 191536  | **Symptom/Scenario:** When the switch is rebooted with an SVI shutdown, if the IP address is changed and the SVI re-enabled, the old VLAN IP address still replies to an ARP request received.  
**Workaround:** Delete and then add back the SVI. |
| Credential Manager| 94938   | **Symptom:** During boot, the following message is observed, after which the features to not function:  
```
---------------------------------------------------------------------
... ...
[OK] Starting HPE Credential Manager.
... ...
[FAILED] Failed to start HPE Credential Manager.
See 'systemctl status hpe-credmgr.service' for details.
[DEPEND] Dependency failed for Halon NTP Helper Daemon
[OK] Stopped HPE Credential Manager.
Starting HPE Credential Manager.
... ...
---------------------------------------------------------------------
```
**Scenario:** If the startup config is large and takes an extensively long time to load or in a VSF environment if members must wait an excessively long time for the conductor to come up or if a hardware failure delays or blocks the VSF role determination for an excessive amount of time, an error message displays during boot and various features do not function after boot.  
**Workaround:** If there is no hardware defect, a power cycle of the switch or entire VSF stack typically resolves the issue. |
| Diagnostics       | 173341  | **Symptom/Scenario:** The IPtraf diagnostic utility does not work.                                                                                                                                               |
| L3 Addressing     | 164817  | **Symptom/Scenario:** The SNMP MIB OID IP-FORWARD-MIB::inetCidrRouteIfIndex returns an invalid output.                                                                                                               |
| MAC Tables        | 86543, 154852, 159156, 190398 | **Symptom:** Traffic in a VSX pair is dropped.  
**Scenario:** When a VSX pair is in VRRP BACKUP/BACKUP mode, traffic using VRRP MAC as the destination MAC that hits the VSX pair will be dropped. |
| sFlow             | 151822  | **Symptom:** The sFlow sampled packets from a LAG contain the ifIndex of the member port instead of the LAG itself.  
**Scenario:** When sFlow sampling is enabled on a LAG interface, the sFlow sampled packets from the LAG contain the ifIndex of the member port rather than the ifIndex of the LAG. |
## Feature Caveats

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| BGP                                          | In a multi-VRF environments, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example:  

```plaintext
! route-map rmap permit seq 10
    set local-preference 50
!
router bgp 100
    vrf red
        neighbor 1.1.1.2 remote-as 100
        address-family ipv4 unicast
        neighbor 1.1.1.2 activate
        neighbor 1.1.1.2 route-map rmap in
        exit-address-family
```

In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes. |
<p>| Classifiers                                  | Classifier policies, IPv6 and MAC ACLs are not supported on egress.                                                                                                                                              |
| Classifiers                                  | Egress ACL logging is not supported.                                                                                                                                                                              |
| 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                                  | IPv4 egress ACLs can be applied only to route-only ports.                                                                                                                                                        |
| Classifiers                                  | Policies containing both MAC and IPv6 classes are not allowed.                                                                                                                                                    |
| CMF                                          | Automatic downgrade of the startup-config is not supported during a software downgrade. To restore a configuration use the procedure documented under <a href="#">Manual configuration restore for software downgrade</a>. |
| CMF                                          | No other checkpoint besides &quot;startup-configuration&quot; gets migrated during the upgrade process.                                                                                                                     |
| Counters                                     | Layer 3 Route-only port counters are not enabled by default. Enabling them will reduce ipv4 route scale to 80K.                                                                                                   |
| ICMP Redirect                                | The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.                                                                                                                                   |
| IGMP/PIM on Loopback and GRE interfaces      | IGMP cannot be enabled on both Loopback and GRE interfaces. PIM can be enabled on a Loopback interface. PIM will not work on GRE tunnels and 6in6.                                                              |
| Multicast                                    | Multicast traffic with a Null Source IP (0.0.0.0) gets flooded.                                                                                                                                                  |
| MVRP and VSX                                 | MVRP is mutually exclusive with VSX.                                                                                                                                                                             |
| Network Analytics Engine (NAE)               | Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.                                                                          |
| Network Analytics Engine (NAE)               | Network Analytics Engine (NAE) agents execute Command Line Interface (CLI)                                                                                                                                        |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Analytics Engine (NAE)</td>
<td>The following tables are not supported for NAE scripts: OSPF Route, OSPF LSA, OSPF Neighbor, BGP Route.</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPFv2 and OSPFv3 do not support detailed LSA show commands.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Authorization by means of HPE VSAs is not supported.</td>
</tr>
<tr>
<td>REST</td>
<td>REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.</td>
</tr>
<tr>
<td>RIP/RIPng</td>
<td>Redistribute RIP/RIPng is not supported in BGP/BGP+.</td>
</tr>
<tr>
<td>RIP/RIPng</td>
<td>RIP/RIPng metric configuration support is not available.</td>
</tr>
<tr>
<td>RPVST+ and MSTP</td>
<td>Spanning Tree can only run in MSTP or RPVST+ mode.</td>
</tr>
<tr>
<td>RPVST+ and MVRP</td>
<td>RPVST+ is mutually exclusive with MVRP.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF names are limited to 31 characters.</td>
</tr>
<tr>
<td>VRRP</td>
<td>The same virtual link-local address cannot be used across different VRFs.</td>
</tr>
<tr>
<td>VRRP-MD5 authentication interoperability</td>
<td>Not supported with Comware-based switches</td>
</tr>
<tr>
<td>VRRP</td>
<td>VRRP Preemption Delay Timer (preempt delay minimum) may be ignored after a switch reboot or power cycle.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 Routes</td>
<td>215070</td>
<td><strong>Symptom</strong>: Routing failed due to the SVI in shutdown state. <strong>Scenario</strong>: Inter-VLAN traffic is affected due to the presence of a neighbor for the shutdown L3 VLAN. This caused the traffic to take the L3 path rather than the L2L2/ route path. <strong>Workaround</strong>: Remove the shutdown L3 VLAN.</td>
</tr>
</tbody>
</table>
| REST              | 203600 | **Symptom**: A main distribution frame (MDF) switch did not correctly
<table>
<thead>
<tr>
<th>Category</th>
<th>Bug ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| OSPF     | 149301 | **Symptom:** The switch shows unexpected behavior in the OSPFv2/3 DLOGs.  
**Scenario:** When `debug ospfv2 packet` or `debug ospfv3 packet` is enabled with the `ip` filter, the switch shows unexpected behavior in the OSPFv2/3 DLOGs.  
**Workaround:** Use `debug ospfv2 packet` or `debug ospfv3 packet` with the `port` filter and `grep` for the required IP (v4 or v6) address. |
| OSPF     | 160179 | **Symptom/Scenario:** ABR does not inject the default route in a Totally Stubby Area with loopback in Area 0.0.0.0.  
**Workarounds:** Assign one or more physical interfaces to Area 0.0.0.0. |

**Upgrade information**

Version 10.08.1060 uses ServiceOS TL.01.08.0002.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00xx version of software to 10.09.xx.x.

To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where `<VLAN_ID>` is the native VLAN ID configured on the trunk interface.

If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

10.06 is the minimum required software version prior to upgrading to 10.08. If your device is using a version of software prior to 10.06, you must first upgrade to a version of 10.06 before upgrading to 10.08. Check release notes for the software version you will upgrade to for instructions on performing the upgrade to 10.06.

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

When upgrading from software versions before 10.05.0001, if the switch is configured with an entry in a classmap or an Access List that matches AH or ESP traffic, the policy will fail to apply, as these options are no longer permitted. Remove such entries from the configuration prior to upgrading to 10.08.1060 or remove the respective entries from ACLs or Class that failed to apply after the upgrade to 10.08.1060.
When upgrading from a version of software prior to version 10.05.0001, if the switch is configured with IGMP or MLD snooping options such as “forward”, “fastleave”, “forced-fastleave”, or “blocked” at the VLAN context, after upgrading to this software version, you will need to reconfigure these options for each interface from the interface configuration context.

Example config before 10.05.0001:

```
vlan 2
  ip igmp snooping forward 1/1/1
  ip igmp snooping blocked 1/1/2
  ip igmp snooping force-fastleave 1/1/3
  ip igmp snooping fastleave 1/1/4
```

Example config to be added after upgrade to this software version:

```
interface 1/1/1
  ip igmp snooping forward vlan 2
interface 1/1/2
  ip igmp snooping blocked vlan 2
interface 1/1/3
  ip igmp snooping force-fastleave vlan 2
interface 1/1/4
  ip igmp snooping fastleave vlan 2
```

Some Network Analytics Engine (NAE) scripts may not function properly after an upgrade. Aruba recommends deleting existing NAE scripts before an upgrade and then reinstalling the scripts after the upgrade. For more information, see the Network Analytics Engine Guide.

**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, TL.10.0x:yyy).
   
   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**
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, 3 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.10.07.0060]
2. Secondary Software Image [xx.10.08.1060]

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 2017-2022 Hewlett Packard Enterprise Development LP

RESTRICTED RIGHTS LEGEND

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.
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.