



HPE Aruba Networking EdgeConnect Resolution to Multiple OpenSSL CVEs

Instructions for vulnerability resolution for EdgeConnect appliances running ECOS software and EdgeConnect Orchestrator running in all deployment modes.

Aruba Product Security Advisory ID: **ARUBA-PSA-2023-001**

CVE: CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286

CVE-2023-2650 added with version 2

Version 1.0 – Initial Release

Version 1.1 – released April 5, 2023

Version 1.2 – released May 17, 2023 (Updated Orchestrator and ECOS Release status)

Version 2 – released August 21, 2023 as an addendum covering CVE-2023-2650 (Updated RPM file, Orchestrator and ECOS Releases)

Contents

- EdgeConnect Orchestrator 2
 - Vulnerable Orchestrator Releases:**..... 2
- Security Resolution for Orchestrator 2
 - Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, On Prem, Existing Deployments 2
 - Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, On Prem, New Deployments..... 4
 - Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, Public Cloud IaaS..... 4
 - Existing customers deployed in AWS 4
 - New customers deploying in AWS 4
 - Existing customers deployed in Azure or Google Cloud Platform (GCP) 4
 - New Customers deploying in Azure or GCP 5
 - Aruba EdgeConnect Enterprise Orchestrator-as-a-Service (OaaS)..... 6
 - Enterprise, Single Tenant OaaS..... 6
 - Orchestrator Global Enterprise Tenant OaaS instances..... 6
 - Orchestrator-SP Tenant OaaS 7
- EdgeConnect OS (ECOS)..... 8
 - Vulnerable ECOS releases:..... 8
- Resolution for EdgeConnect OS (ECOS) 8

The instructions listed below are to address Aruba Product Security Advisory ID: ARUBA-PSA-2023-001 which covers the following CVEs:

- CVE-2022-4304
- CVE-2022-4450
- CVE-2023-0215
- CVE-2023-0286
- This document is updated to cover the additional CVE submissions: CVE-2023-2650

EdgeConnect Orchestrator

Vulnerable Orchestrator Releases:

Orchestrator Model	Deployment Model	Affected Releases
Aruba EdgeConnect Enterprise Orchestrator	Self-hosted On Prem	All existing Orchestrator instances are affected regardless of release.
	Self-hosted Public Cloud IaaS	
Aruba EdgeConnect Enterprise Orchestrator-as-a-Service (OaaS)	Enterprise, Single Tenant OaaS	
	Orchestrator-SP Tenant OaaS	
	Orchestrator Global Enterprise Tenant OaaS	

Security Resolution for Orchestrator

Depending on the Orchestrator deployment mode, actions must be completed as detailed here.

Self-hosted Orchestrators must have OpenSSL patched either by installing an RPM package or running yum update depending on the deployment model. Upgrading the Orchestrator application does not resolve these vulnerabilities.

Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, On Prem, Existing Deployments

Existing customers with self-hosted, on-prem VM running CentOS Linux 7.9.2009:

Instructions:

1. Download RPM package from [Aruba Support Portal](#), as shown in the following figure. The file name is 'Orchestrator CentOS RPM 2023_06_15'. The zip file contains the install script "install_orchestrator_rpms.sh."



Special instructions for security advisory remediation; addendum covering CVE-2023-2650

Showing 2 Results

Sort by: Relevance

File Category: RPM Clear All

Orchestrator_CentOS_RPM_2023_06_15.zip
Aruba EdgeConnect Enterprise v-- Aruba EdgeConnect SD-WAN Orchestration Software ECOS
Released on Jul 26, 2023 RPM 1.71 MB

Orchestrator CentOS RPM 2023_03_13
Aruba EdgeConnect Enterprise v-- Aruba EdgeConnect SD-WAN Orchestration Software
Released on Mar 28, 2023 RPM 1.79 MB

2. Choose one of these options:

- Download the `Orchestrator_CentOS_RPM_<*>.zip` from ASP directly in the orchestrator using `wget` command.
- Download the `Orchestrator_CentOS_RPM_<*>.zip` locally to any server and secure copy (`scp`) the RPM package to a directory on Orchestrator such as `/tmp`. From within Orchestrator, files can be copied from an external server using `scp`. To use `scp`, refer to the following procedure:
<https://www.arubanetworks.com/techdocs/sdwan/docs/orch/orchestrator/sw-setup/upgrade-orch/#upgrade-via-scp>

3. Verify the SHA 256 checksum of the downloaded zip file and ensure it matches the published checksum in ASP.

4. In Orchestrator, log in and enter `'su -'` to become root user.

5. Unzip the RPM package; observe the following output:

```
root@orchestrator:/root$ unzip Orchestrator_CentOS_RPM_2023_06_15.zip
Archive:  Orchestrator_CentOS_RPM_2023_06_15.zip
  creating:  orchestrator_rpms/
 inflating:  orchestrator_rpms/openssl-1.0.2zh-2.e17.x86_64.rpm
 inflating:  orchestrator_rpms/openssl-libs-1.0.2zh-2.e17.x86_64.rpm
 inflating:  install_orchestrator_rpms.sh
```

6. Install the RPM package; observe the following output:

```
root@orchestrator:/root$ ./install_orchestrator_rpms.sh
Preparing...                               ##### [100%]
Updating / installing...
 1:openssl-libs-1:1.0.2zh-2.e17            ##### [ 25%]
 2:openssl-1:1.0.2zh-2.e17                 ##### [ 50%]
Cleaning up / removing...
 3:openssl-1:1.0.2k-26.e17_9               ##### [ 75%]
 4:openssl-libs-1:1.0.2k-26.e17_9         ##### [100%]
```

7. Verify correct OpenSSL version by running the command:

```
root@orchestrator:/root$ openssl version
```



Special instructions for security advisory remediation; addendum covering CVE-2023-2650

- The expected output should be: `OpenSSL 1.0.2zh-fips 30 May 2023`
- Given that OpenSSL has been explicitly updated, the Orchestrator application does not need to be updated. However, the customer may choose to update the Orchestrator application to have access to new/updated features and/or other security updates.

Note: Customers running Fedora OS must upgrade to CentOS for general support of security updates. Contact Customer Support for the procedure.

Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, On Prem, New Deployments

Orchestrator virtual installation packages that contain the fix include:

Build	Availability Date
9.1.8.40019	Aug 4, 2023, as First Customer Ship (FCS)
9.2.6.40033	Aug 4, 2023, as FCS
9.3.1.xxxxx	9.3.1.xxxxx is planned for release as FCS by the end of August 2023

If the new instance is deployed before these releases are available, customers can deploy existing versions and run the RPM updates as described above.

Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, Public Cloud IaaS

Customers should complete the steps in the following section that matches their IaaS deployment.

Existing customers deployed in AWS

Instructions:

- Run `'yum update'` on the EC2 Orchestrator instance.

The Orchestrator application does not need to be updated. However, the customer may choose to update the Orchestrator application to have access to new/updated features and/or other security updates.

New customers deploying in AWS

No additional action required. Deploy the new Orchestrator as documented here: <https://www.arubanetworks.com/techdocs/sdwan/deployments/>

Existing customers deployed in Azure or Google Cloud Platform (GCP)

Instructions:

Download **RPM package** from [Aruba Support Portal](#). Follow the procedure that is detailed in [Aruba EdgeConnect Enterprise Orchestrator, Self-hosted, On Prem, Existing Deployments](#).

Given that OpenSSL has been explicitly updated via the RPM package, the Orchestrator application does not need to be updated. However, the customer may choose to update the Orchestrator application to have access to new/updated features and/or other security updates.



New customers deploying in Azure or GCP

1. Deploy Orchestrator **8.10.23_updated2** from the IaaS marketplace.
 - a. Available in Azure now. Ensure **v8.10.23_updated2** is selected since prior releases are retained for 90 days and therefore are still in the pull-down list.

The screenshot shows the Azure Marketplace page for Silver Peak Unity Orchestrator. The page includes a navigation bar with 'Azure Marketplace', 'Apps', and 'Consulting Services'. The main content area displays the product name, version, and license type. The version 'v8.10.23_updated2' is highlighted with a red box, and the license type 'BYOL' is also visible. The page also includes a 'Get It Now' button and a list of categories and support options.

Product Name	License Type
Silver Peak Unity Orchestrator v8.10.23_updated	BYOL
Silver Peak Unity Orchestrator v8.10.23_updated2	BYOL
Silver Peak Unity Orchestrator v8.10.23_updated	BYOL

- b. Available in GCP now.



2. Once the Orchestrator is deployed from the marketplace, the Orchestrator application can be upgraded to 9.1, 9.2, or 9.3 per customer requirements.

Aruba EdgeConnect Enterprise Orchestrator-as-a-Service (OaaS)

Orchestrator-as-a-Service (OaaS) Releases that resolve the OpenSSL CVEs

Orchestrator 9.3.1 and above	9.3.1.xxxxx is planned for release as FCS by the end of August 2023
-------------------------------------	---------------------------------------------------------------------

Note: Orchestrator Releases 8.x.y and 9.0.y are affected and are out of maintenance. OaaS Customers must upgrade to one of the releases listed above.

Enterprise, Single Tenant OaaS

If OaaS release is lower than 9.2.2, then open a TAC case to upgrade per the table above.

If release is 9.2.2 or later, then enterprise customers can self-upgrade to 9.3.1 (or later releases).

Orchestrator Global Enterprise Tenant OaaS instances

If OaaS tenant orchestrator release is lower than 9.2.2, then open a TAC case to upgrade per the table above.

If the tenant orchestrator is running release is 9.2.2 or later, Orchestrator Global Enterprise customers can self-upgrade tenant orchestrators to 9.3.1 (or later releases).



Orchestrator-SP Tenant OaaS

Global Service Providers running Orchestrator-SP must coordinate upgrades of tenant orchestrators to 9.3.1 (or later releases) as soon as possible.



EdgeConnect OS (ECOS)

Vulnerable ECOS releases:

Vulnerable Aruba EdgeConnect Enterpriser releases:

ECOS 9.2.x.x release stream: ECOS 9.2.5.0 and below

ECOS 9.1.x.x release stream: ECOS 9.1.7.x and below

ECOS 9.0.x.x release stream: ECOS 9.0.x.x and below

ECOS 8.x.x.x release stream: ECOS 8.3.x.x and below

Note ECOS Release 8.3.x and 9.0.x are affected and are out of maintenance.

Resolution for EdgeConnect OS (ECOS)

ECOS Releases that resolve the OpenSSL CVEs

ECOS 9.3.1.0 and above	ECOS 9.3.1 is planned to be released by the end of August, 2023
ECOS 9.2.6.0 and above	ECOS 9.2.6.0 is planned to be released by the end of August, 2023
ECOS 9.1.8.0 and above	ECOS 9.1.8.0 is planned to be released by the end of August, 2023

Note: ECOS Release 8. x and 9.0.x are affected and are out of maintenance. Upgrade to one of the ECOS 9.1.x are above release streams.

[Explore HPE GreenLake](#)



© Copyright 2023 Hewlett Packard Enterprise Development LP. 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.

All third-party marks are property of their respective owners.