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

Version 1.0 – Initial Release, March 14, 2023

Version 1.1 – Released April 5, 2023

Version 1.2 – Released May 17, 2023 (Updated Orchestrator and ECOS release status)

Contents

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

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_03_13.zip*'. The zip file contains the install script "install_orchestrator_rpms.sh."

Special instructions for security advisory remediation

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_03_13.zip
Archive:  Orchestrator_CentOS_RPM_2023_03_13.zip
  creating: orchestrator_rpms/
  inflating: orchestrator_rpms/openssl-1.0.2zg-2.el7.x86_64.rpm
  inflating: orchestrator_rpms/openssl-libs-1.0.2zg-2.el7.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-1:1.0.2zg-2.el7     ################################# [ 25%]
   2:openssl-1:1.0.2zg-2.el7          ################################# [ 50%]
Cleaning up / removing...
   3:openssl-1:1.0.2k-25.el7_9        ################################# [ 75%]
   4:openssl-libs-1:1.0.2k-25.el7_9   ################################# [100%]
```

7. Verify correct OpenSSL version by running the command:

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

8. The expected output should be: OpenSSL 1.0.2zg-fips 13 Feb 2023
9. 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 **OVA 9.1.7, 9.2.4, and 9.3.0** will contain the fixes and will be available in the beginning of May 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:

1. 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)

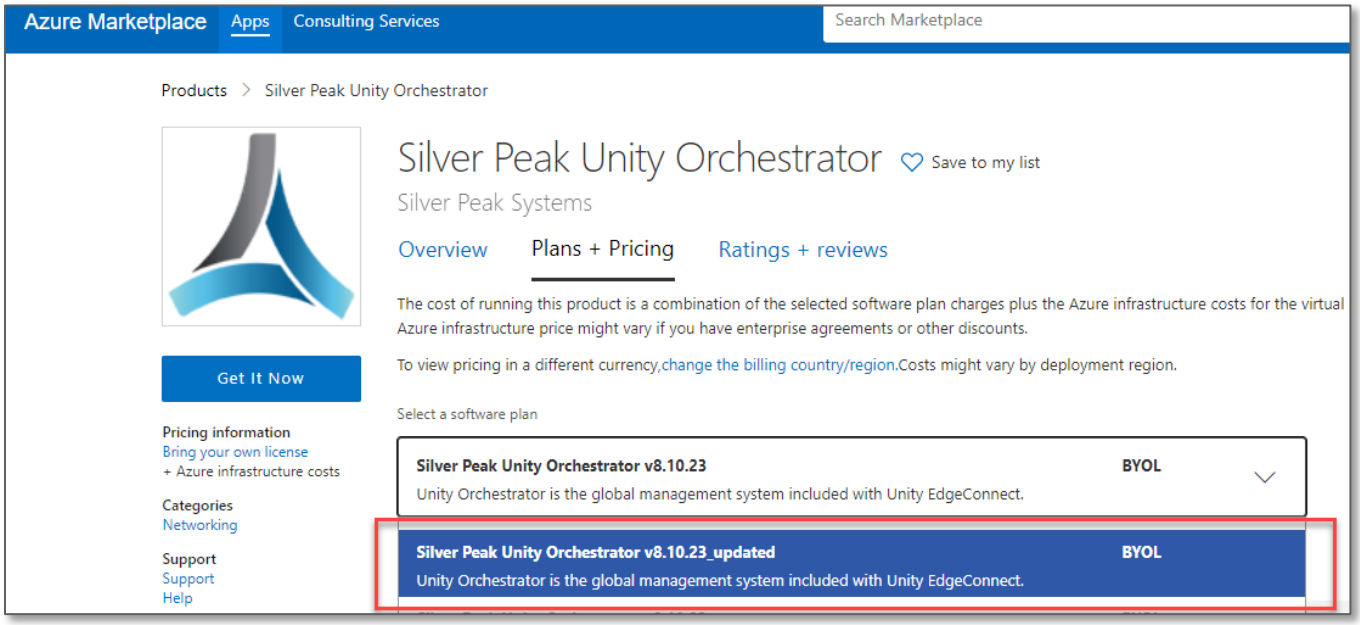
Instructions:

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



b. Availability in GCP is expected the first week April 2023.

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 **9.3.0** and above	Available Now: 9.3.0.41159 was released as FCS May 13, 2023
Orchestrator **9.2.4** and above	Available Now: 9.2.4.40091 was released as GA April 13, 2023
Orchestrator **9.1.7** and above	Available Now: 9.1.7.40101 was released as FCS May 11, 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 9.2.4 or 9.3.0 (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 9.2.4 or 9.3.0 (or later releases).

Orchestrator-SP Tenant OaaS

Global Service Providers running Orchestrator-SP must coordinate upgrades of tenant orchestrators to 9.2.4 or 9.3.0 (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 9.2.3.0 and below

ECOS 9.1.x.x release stream: ECOS 9.1.5.0 and below

ECOS 9.0.x.x release stream: ECOS 9.0.8.0 and below

ECOS 8.x.x.x release stream: ECOS 8.3.8.0 and below

Note: ECOS Release 8.3.x is affected and is out of maintenance.

Resolution for EdgeConnect OS (ECOS)

ECOS Releases that resolve the OpenSSL CVEs

ECOS 9.3.0.0 and above	Available Now: ECOS 9.3.0.0_95721 was released as FCS May 12, 2023
ECOS 9.2.4.0 and above	Available Now: ECOS 9.2.4.0_94654 was released as FCS May 15, 2023
ECOS 9.1.6.0 and above	Available Now: ECOS 9.1.6.0_92628 was released as FCS May 15, 2023
ECOS 9.0.9.0 and above	Available Now: ECOS 9.0.9.0_90419 was released as FCS April 28, 2023

Notes:

1. ECOS Release 8.x is affected and is out of maintenance. Upgrade to one of the ECOS 9.x releases.
2. EdgeConnect product management recommends 9.1 or above because 9.0 will become end of maintenance as of June 30, 2023.