HPE Aruba Networking EdgeConnect SD-WAN Orchestrator

Resolution to CVE-2024-6387

Instructions for vulnerability resolution for EdgeConnect SD-WAN Orchestrator in self-hosted/on-prem deployment models.

A new Remote Code Execution vulnerability was discovered in OpenSSH

HPE Product Security Advisory ID: **HPESBNW04669** published July 15, 2024

CVE: CVE-2024-6387

Version 1.0 – Initial Release, July 15, 2024

Contents

EdgeConnect SD-WAN Orchestrator Deployment Models

Vulnerable Orchestrator Releases

Orchestrator Model	Deployment Model	Affected Releases
HPE Aruba Networking EdgeConnect SD-WAN Orchestrator	Self-hosted On Prem	All existing Orchestrator instances running Rocky Linux are affected regardless of release. Orchestrators running CentOS 7 are not affected.
	Self-hosted Public Cloud IaaS	Self-hosted Orchestrators running Rocky Linux in Azure and Google Cloud Platform (GCP) are affected. Self-hosted Orchestrators running Cent OS in Azure and Google Cloud Platform (GCP) are not affected. Self-hosted Orchestrators running in AWS are not affected.
Aruba EdgeConnect Orchestrator-as-a-Service (OaaS)	Enterprise, Single Tenant OaaS	OaaS is not affected
	Orchestrator-SP Tenant OaaS	Orchestrator-SP tenant Orchestrators are not affected
	Orchestrator Global Enterprise Tenant OaaS	Orchestrator Global Enterprise tenant Orchestrators are not affected

NOTE: EdgeConnect OS (ECOS) is not affected by this CVE.

Security Resolution for Orchestrator

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

Affected self-hosted Orchestrators must have OpenSSH patched either by running yum update or by installing an RPM package depending on the deployment model and/or customer environment.

Upgrading the Orchestrator application does not resolve this vulnerability.

HPE Aruba Networking recommends that customers running Fedora OS or CentOS 7 should upgrade to Rocky Linux as soon as possible for general support of Linux security updates as these releases have reached End of Support. Contact Customer Support for the procedure.

EdgeConnect SD-WAN Orchestrator, Self-hosted, On Prem, Existing Deployments, Yum Update Method

1. In Orchestrator, log in and become root user by entering '**`su –`**' and the root user password.

2. Run '**`yum update -y openssh`**' on the Orchestrator instance. If "yum update" hasn't been run for awhile, it is recommended to run a full yum update.

```
root@orchestrator:/root$ yum update -y openssh
Last metadata expiration check: 0:00:29 ago on Mon 08 Jul 2024 10:32:18 AM
PDT.
Dependencies resolved.
================================================================================
 Package                                Architecture                Version
Repository                   Size
================================================================================
Upgrading:
   openssh x86_64  8.7p1-38.el9_4.1 baseos  458 k
   openssh-clients  x86_64  8.7p1-38.el9_4.1 baseos  713 k
   openssh-server  x86_64  8.7p1-38.el9_4.1 baseos  459 k

Transaction Summary
================================================================================
Upgrade  3 Packages
Total download size: 1.6 M
Downloading Packages:
(1/3): openssh-server-8.7p1-38.el9_4.1.x86_64.rpm   870 kB/s | 459 kB 00:00
(2/3): openssh-8.7p1-38.el9_4.1.x86_64.rpm          832 kB/s | 458 kB 00:00
(3/3): openssh-clients-8.7p1-38.el9_4.1.x86_64.rpm  992 kB/s | 713 kB 00:00
--------------------------------------------------------------------------------
Total      1.7 MB/s | 1.6 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing: 1/1
Running scriptlet: openssh-8.7p1-38.el9_4.1.x86_64  1/6
```

```
Upgrading  :       openssh-8.7p1-38.el9_4.1.x86_64  1/6
```

Output removed for brevity

```
Cleanup    openssh-8.7p1-34.el9.x86_64      6/6
Running scriptlet: openssh-8.7p1-34.el9.x86_64      6/6
Verifying  openssh-server-8.7p1-38.el9_4.1.x86_64   1/6
Verifying  openssh-server-8.7p1-34.el9.x86_64       2/6
Verifying  openssh-clients-8.7p1-38.el9_4.1.x86_64  3/6
Verifying  openssh-clients-8.7p1-34.el9.x86_64      4/6
Verifying  openssh-8.7p1-38.el9_4.1.x86_64  5/6
Verifying  openssh-8.7p1-34.el9.x86_64      6/6

Upgraded:
   openssh-8.7p1-38.el9_4.1.x86_64
   openssh-clients-8.7p1-38.el9_4.1.x86_64
   openssh-server-8.7p1-38.el9_4.1.x86_64

Complete!
root@orchestrator:/root$
```

3. Verify openssh package version “8.7p1-38.el9_4.1”. The “_4.1” is what changes with the new version.

```
root@orchestrator:/root$ rpm -q openssh openssh-server
openssh-8.7p1-38.el9_4.1.x86_64
openssh-server-8.7p1-38.el9_4.1.x86_64
```

4. Verify openssh package version “8.7p1-38” CVE Resolution

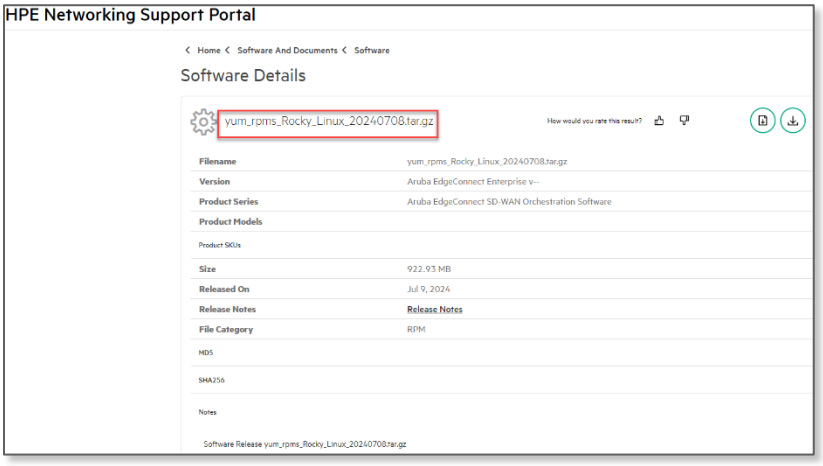
```
root@orchestrator:/root$ rpm -q --changelog openssh | grep -B1 CVE-2024-6387
* Fri Jun 28 2024 Dmitry Belyavskiy <dbelyavs@redhat.com> - 8.7p1-38.1
- Possible remote code execution due to a race condition (CVE-2024-6387)
```


EdgeConnect SD-WAN Orchestrator, Self-hosted, On Prem, Existing Deployments, RPM Method

For customers with restricted environments that can not run yum update, HPE Aruba Networking has provided an RPM package on the HPE Networking Support Portal.

1. Download RPM package from HPE Networking Support Portal.

   The file name is '***yum_rpms_Rocky_Linux_20240708.tar.gz***'.
   https://networkingsupport.hpe.com/downloads/software/RmlsZTo5NWFlNjY2NC0zZjQzLTExZWYtOWYzZS05ZjQzN2RmYjE1YmU%3D
   The zip file contains the install script "install_orchestrator_rpms.sh."



2. Choose one of these options:
   - Download the ***yum_rpms_Rocky_Linux_20240708.tar.gz*** file from ASP directly in the orchestrator using wget command.
   - Download the ***yum_rpms_Rocky_Linux_20240708.tar.gz*** 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 become root user by entering '**`su -`**' and the root user password.
5. Unzip the RPM package; observe the following output:

   ```
   root@orchestrator:/root$ tar -xf /tmp/yum_rpms_Rocky_Linux_20240708.tar.gz


   root@orchestrator:/root$ cd yum
   ```

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

   ```
   root@orchestrator:/root/yum$ yum install -y openssh*.rpm
   ==========================================================================
   ```

```
Package    Architecture    Version Repository      Size
================================================================================
Upgrading:
openssh    x86_64   8.7p1-38.el9_4.1 @commandline    458 k
openssh-clients    x86_64   8.7p1-38.el9_4.1 @commandline    713 k
openssh-server     x86_64   8.7p1-38.el9_4.1 @commandline    459 k

Transaction Summary
================================================================================
Upgrade  3 Packages

Total size: 1.6 M
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :       1/1
  Running scriptlet: openssh-8.7p1-38.el9_4.1.x86_64        1/6
  Upgrading        : openssh-8.7p1-38.el9_4.1.x86_64        1/6
```

Output removed for brevity

```
  Cleanup          : openssh-8.7p1-34.el9.x86_64    6/6
  Running scriptlet: openssh-8.7p1-34.el9.x86_64    6/6
  Verifying        : openssh-8.7p1-38.el9_4.1.x86_64        1/6
  Verifying        : openssh-8.7p1-34.el9.x86_64    2/6
  Verifying        : openssh-clients-8.7p1-38.el9_4.1.x86_64        3/6
  Verifying        : openssh-clients-8.7p1-34.el9.x86_64    4/6
  Verifying        : openssh-server-8.7p1-38.el9_4.1.x86_64 5/6
  Verifying        : openssh-server-8.7p1-34.el9.x86_64     6/6

Upgraded:
openssh-8.7p1-38.el9_4.1.x86_64
```


```
openssh-clients-8.7p1-38.el9_4.1.x86_64
openssh-server-8.7p1-38.el9_4.1.x86_64

Complete!
```

7. Verify correct OpenSSH version:

```
root@orchestrator:/root/yum$ rpm -q --changelog openssh | grep -B1 CVE-2024-6387
* Fri Jun 28 2024 Dmitry Belyavskiy <dbelyavs@redhat.com> - 8.7p1-38.1
- Possible remote code execution due to a race condition (CVE-2024-6387)
```

8. Clean up unneeded files

```
root@orchestrator:/root/yum$ cd
root@orchestrator:/root$ rm -fr /tmp/yum_rpms*.tar.gz yum rpms_manifest.txt
```

Given that OpenSSH 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.

EdgeConnect SD-WAN Orchestrator, Self-hosted, On Prem, New Deployments

It is recommended to run yum update on all new Orchestrator installations to ensure the patch is included.