

**Date: September 9th, 2020**

**Version: 1.0**

Revision	Date	Changes
1.0	September 9th, 2020	Initial Release

The CVE-ID tracking this issue is: CVE-2020-24333

CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

## Description

This advisory documents the impact of a vulnerability in Arista's CloudVision Portal (CVP). The effect of this vulnerability is that users with "read-only" or greater access rights to the Configlet Management module can download files not intended for access, located on the CVP server, by accessing a specific API. This API can only be accessed by authenticated users.

The access rights of a given user are based on the user's assigned role. "network-operators" have "read-only" access rights to all modules (including Configlet Management) and any user with a network-operator role is therefore affected. The "network-admins" role is affected as well due to its access rights to all modules. If a custom role has been configured, the associated access rights can be viewed by opening the `/cv/settings/aaa-roles` URL on the CVP Web GUI.

Example:

The following steps detail how the access rights for a user "test\_user" with role "Test Role" can be viewed from the CVP Web GUI:

1) Check the assigned role(s) for a given user from `/cv/settings/aaa-users`:

<input type="checkbox"/>	User	First Name	Last Name	Email	Authentication Type	Roles	User Status	Current Status
	test_user	Filter	Filter	Filter	Filter	Filter	Filter	Filter
<input checked="" type="checkbox"/>	test_user			test_user@domain.com	Local	Test Role	Enabled	Offline

2) View the access rights of the concerned role from `/cv/settings/aaa-roles`:

Name\* :

Test Role

Description (optional) :

Test User Role

Module Access

Inventory

Inventory Management

Read Only

▼

vEOS Router Management

Read Only

▼

Provisioning

Change Control Approval

Read Only

▼

Change Control Management

Read Only

▼

Configlet Management

Read Only

▼

Image Management

Read Only

▼

Network Provisioning

Read Only

▼

Public Cloud Accounts

Read Only

▼

Snapshot

Read Only

▼

Tag Management

Read Only

▼

Task Management

Read Only

▼

Workflow

Read Only

▼

Zero Touch Provisioning

Read Only

▼

Settings

AAA Settings

Read Only

▼

Account Management

Read Only

▼

Audit Logs

Read Only

▼

Cluster Management

Read Only

▼

Licensing

Read Only

▼

SSL

Read Only

▼

Events

Event Acknowledgment

Read Only

▼

Event Configuration

Read Only

▼

Event Notification

Read Only

▼

Telemetry

Bug Alerts Management

Read Only

▼

Metric Dashboards

Read Only

▼

Multi-switch Tap Aggregation

Read Only

▼

This vulnerability was discovered internally and there has been no report of exploitation in the field.

Vulnerability Assessment

Affected Software

--

CloudVision Portal
All releases prior to 2020.2

## Affected Platforms

- This vulnerability affects CloudVision virtual and physical appliances running with the versions identified above.
- The following products are **not affected**:
  - CloudVision as-a-Service
  - EOS running on Arista switching platforms
  - CloudEOS VM / vEOS Router
  - Arista Wireless Access Points
  - Arista 7130 Systems running MOS
  - Big Switch Nodes for BCF and BMF (Arista CCF and DMF)

## Mitigation

For custom roles, access to the Configlet Management Module can be disabled by navigating to **Settings/Access Controls/Roles/Role\_name** on the CVP Web GUI and selecting “No Access” as indicated below:

Name* :	<input type="text" value="Test Role"/>	Description (optional) :	<input type="text" value="Test User Role"/>
---------	--	--------------------------	---

  

Module Access			
Inventory		Settings	
Inventory Management	<input type="text" value="Read Only"/>	AAA Settings	<input type="text" value="Read Only"/>
vEOS Router Management	<input type="text" value="Read Only"/>	Account Management	<input type="text" value="Read Only"/>
Provisioning		Audit Logs	<input type="text" value="Read Only"/>
Change Control Approval	<input type="text" value="Read Only"/>	Cluster Management	<input type="text" value="Read Only"/>
Change Control Management	<input type="text" value="Read Only"/>	Licensing	<input type="text" value="Read Only"/>
Configlet Management	<input type="text" value="No Access"/>	SSL	<input type="text" value="Read Only"/>
Image Management	<input type="text" value="Read Only"/>	Events	
Network Provisioning	<input type="text" value="Read Only"/>	Event Acknowledgment	<input type="text" value="Read Only"/>
Public Cloud Accounts	<input type="text" value="Read Only"/>	Event Configuration	<input type="text" value="Read Only"/>
Snapshot	<input type="text" value="Read Only"/>	Event Notification	<input type="text" value="Read Only"/>
Tag Management	<input type="text" value="Read Only"/>	Telemetry	
Task Management	<input type="text" value="Read Only"/>	Bug Alerts Management	<input type="text" value="Read Only"/>
Workflow	<input type="text" value="Read Only"/>	Metric Dashboards	<input type="text" value="Read Only"/>
Zero Touch Provisioning	<input type="text" value="Read Only"/>	Multi-switch Tap Aggregation	<input type="text" value="Read Only"/>

Please note that module access cannot be disabled for default roles “network-operator” and “network-admin”. The above mitigation step applies to custom roles alone. For the resolution, please refer to the next section which lists the details of the remediated software versions.

## Resolution

This vulnerability is being tracked by Bug 502053 and has been addressed in the 2020.1.2, 2020.2.0 and later versions of CloudVision Portal. The recommended resolution is to upgrade to a version of CloudVision Portal with the fix included.

### For More Information:

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

### Open a Service Request:

By email: [support@arista.com](mailto:support@arista.com)

By telephone: 408-547-5502

866-476-0000