Date: July 26th, 2022

Revision	Date	Changes
1.0	July 26th 2022	Initial release

CVE-2022-2907

- The CVE-ID tracking this issue: CVE-2022-29071
- CVSSv3.1 Base Score: 4.0 (AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
- Common Weakness Enumeration (CWE): CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)
- The internal bug tracking this issue: BUG 695468

Description

This advisory documents an internally found vulnerability in the on premises deployment model of Arista CloudVision Portal (CVP) where under a certain set of conditions, user passwords can be leaked in the Audit and System logs.

The impact of this vulnerability is that the CVP user login passwords might be leaked to other authenticated users.

While this advisory is similar to Arista Security Advisory 0045, it is different both in the underlying root cause and in that it discloses the passwords in the audit logs.

This issue is specific to using CVP user authentication via local (user accounts local to CVP application), TACACS or RADIUS, thus only applicable to the on-premises CloudVision Portal; CloudVision as-a-Service does not use these modes of authentication and is not affected by this issue.

This issue was discovered by an Arista customer and Arista is not aware of any malicious use of this issue in customer networks.

Vulnerability Assessment

Affected Software

CloudVision Portal (CVP):

- All releases in the 2020.2 train
- All releases in the 2020.3 train
- All releases in the 2021.1 train
- All releases in the 2021.2 train
- All releases in the 2021.3 train
- 2022.1.0

Affected Platforms

The following CloudVision Portal products are affected with the previously mentioned software versions.

- CloudVision Portal, virtual appliance or physical appliance running CVP

The following product versions and platforms are not affected by this vulnerability:

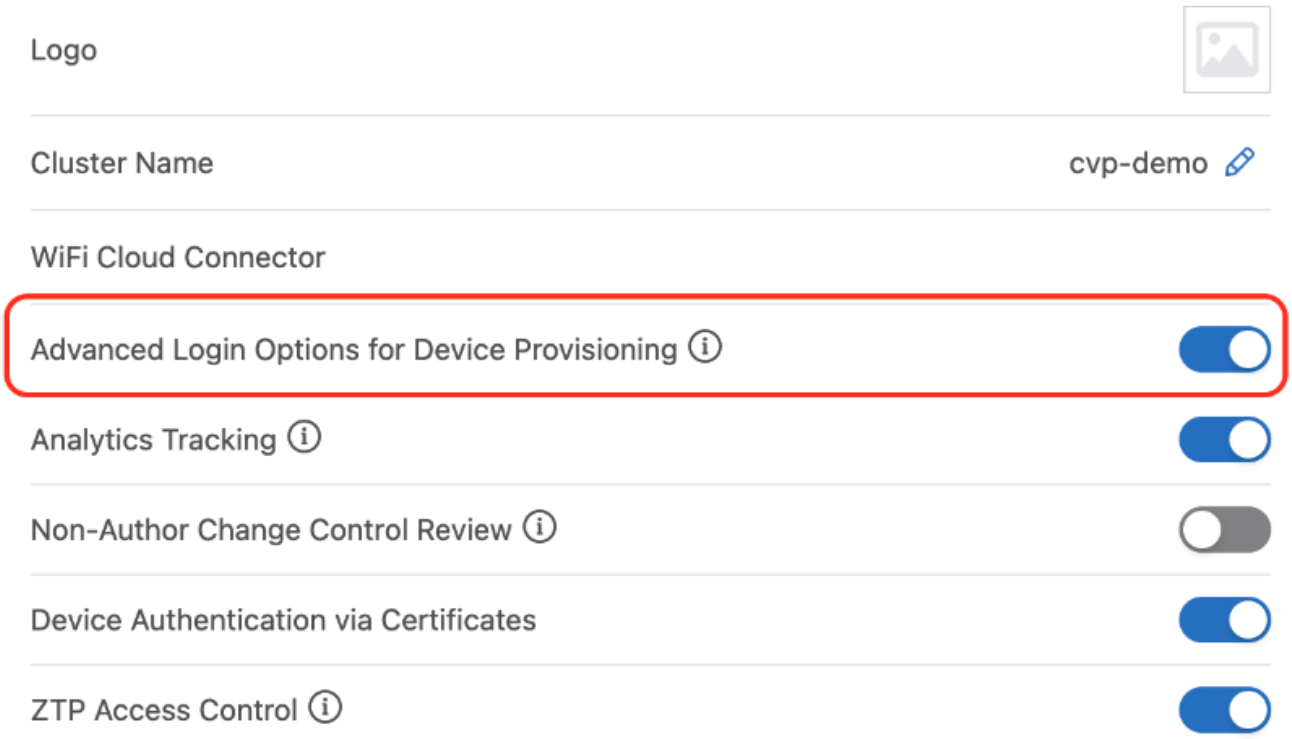
- All Arista EOS-based products (All switching platforms with no exceptions)
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision as-a-Service
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

Required Configuration for Exploitation

In order for this vulnerability to occur, the following conditions must all be met:

1. “Enable” passwords on the switch must be different from the CVP users login passwords
2. Advanced Login Options for Device Provisioning is enabled. This can be verified by navigating to the Settings page and looking for the ‘Advanced login options for device provisioning’ as shown in the screenshot below:

Cluster Management



Indications of Compromise

User passwords will appear in logs.

Mitigation

It is recommended for users logging into CVP to change their password and ensure that it is the same as the enable password on the switch. As a security best practice, it is recommended to restrict access to the CVP application and host operating system to trusted users/user groups and periodically rotate user passwords.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

Hotfix

No hotfix will be made available for this issue.

The following versions contain a fix for this vulnerability

- CVP 2022.1.1
- CVP 2022.2.0 (pending release)

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
By telephone: 408-547-5502 ; 866-476-0000 Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support