Date: February 20, 2024

Revision	Date	Changes
1.0	February 20, 2024	Initial release

CVSSv3.1 Base Score: 9.8 (CVSS:3.1AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-1394 Use of default cryptographic key
This vulnerability is being tracked by BUG 880654

Description

On affected platforms running CloudVision Portal Virtual Appliances on AWS/GCP, a public key is present in the /root/.ssh/authorized_keys file. This key, however, cannot be used unless the accompanying private key is available. While this key is believed to have been deleted, this advisory is being released out of an abundance of caution.

This issue was reported by an external source. Arista is not aware of any malicious uses of this issue in customer networks.

This issue is NOT present in the standard offerings of CloudVision Portal, including:

- CloudVision Portal virtual appliance (as available on arista.com)
- CloudVision Portal physical appliance
- CloudVision as-a-Service

This issue is only present in extremely limited offerings of the Cloudvision Portal virtual appliance software as made available specifically by Arista for unique customer deployments. In particular, a package of CentOS 7.9 combined with CloudVision Portal software was made available to a very limited number of customers.

Vulnerability Assessment

Affected Software

- CVP on AWS
    - AMIs with CentOS version 7.9.2009
- CVP on GCP
    - GCP image with CentOS version 7.9.2009 (crc32c hash: Rvd78A==)

Affected Platforms

The following products **are** affected by this vulnerability:

- CVP on AWS
    - AMIs with CentOS version 7.9.2009 that have the following AMI IDs:
        - ami-00f8e2c955f7ffa9b
        - ami-0a6695f01d82eb4dc
        - ami-00e87074e52e6c9f9
        - ami-020509c0c98a070e8
        - ami-0b2e8350e21023187
- CVP on GCP
    - GCP image with CentOS version 7.9.2009 with crc32c hash: Rvd78A==. Since this image was never released to the public, there is no ID for the image.

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

- CloudVision Portal, when deployed in certain configurations on AWS
    - AMIs with CentOS version below 7.9.2009
- CloudVision Portal, when deployed in certain configurations on GCP
    - GCP image with CentOS version below 7.9.2009

- Arista EOS-based products:
    - 710 Series
    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series

    - 7500E/R/R2/R3 Series
    - 7800R3 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

Required Configuration for Exploitation

In order to be vulnerable to this issue for **AWS** systems, the following conditions must be met:

```
• User must have access to the affected AMI’s as indicated above
```

In order to be vulnerable to this issue for **GCP** systems, the following conditions must be met:

User must have deployed the affected image. This image was not formally released but can be identified in the GCP Storage Bucket UI as having the crc32c hash: Rvd78A==. To check for exposure from the gcloud CLI the following command can be run:

```
$ gsutil stat gs:///centos79-cvp.tar.gz
gs:///centos79-cvp.tar.gz:
    Creation time:          Mon, 29 Nov 2021 11:16:54 GMT
    Update time:            Mon, 29 Nov 2021 11:16:54 GMT
    Storage class:          STANDARD
    Content-Length:         1311712877
    Content-Type:           None
    Component-Count:        5
    Hash (crc32c):            Rvd78A==
    ETag:                   CLnBn6C5vfQCEAE=
    Generation:             1638184614617273
```

```
    Metageneration:          1
```

Mitigation

The workaround for **AWS** is to remove this public key from the /root/.ssh/authorized_keys file. It can be done by running the following command via CLI:

```
sudo sed -i '/tanayam-test-centos-
new-0813/d' /root/.ssh/authorized_keys
```

The workaround for **GCP** is to remove this public key from the /root/.ssh/authorized_keys file. It can be done by running the following command via CLI:

```
sudo sed -i ‘/root@DIEGO-NOTEBOOK/d’ /root/.ssh/authorized_keys
```

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below.

AWS: This issue has been fixed in the following CVP on AWS releases:

- ami-06962ae5e57418c2b
- ami-0f7181a084fa9c47d
- ami-04b81faebe5306237
- ami-009c4a78c07f29db9
- ami-0d36c3fba11991189

GCP: This issue was present in privately-available images only. If you’re affected please contact your SE for a link to an updated version.

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