Date: September 24, 2024

Revision	Date	Changes
1.0	September 24, 2024	Initial release

The CVE-ID tracking this issue: CVE-2024-7142
CVSSv3.1 Base Score: 4.6 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Common Weakness Enumeration: CWE-311: Missing Encryption of Sensitive Data
This vulnerability is being tracked by BUG 984230

Description

On Arista CloudVision Appliance (CVA) affected releases running on appliances that support hardware disk encryption (DCA-350E-CV only), the disk encryption might not be successfully performed. This results in the disks remaining unsecured and data on them being readable without the passphrase. This vulnerability allows local attackers to remove the unencrypted disk from the affected system, then attach to a different system, and access its data.

The issue was discovered internally by Arista. Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

Arista Networks CloudVision Appliance (CVA) Software Versions

- 5.0.2 release and above releases in the 5.0.x train
- 6.0.6 and below releases in the 6.0.x train

Affected Platforms

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

- CloudVision Appliance
  - DCA-350E-CV

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

- 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
    - AWE 7200 Series
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision Appliance platforms
    - DCA-CV-100
    - DCA 200-CV
    - DCA-200-VEOS
    - DCA-250-CV
    - DCA-300-CV
- CloudVision CUE, virtual appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal Virtual Machine image (for virtual appliance or physical appliance)
- CloudVision as-a-Service cloud service delivery
- 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)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

Systems are affected if disk encryption has been enabled using the **cva disk encryption enable** command. Whether a system is currently in the affected configuration can be determined with the following steps.

Preliminary steps

To run the checks described below, it is necessary to run the **racadm** tool in the privileged mode. The tool is available under the **racadm** command in CVA version 5 and 6.

The user will need to know the Fully Qualified Device Descriptor (FQDD) of the RAID controller(s) and the virtual disks. These can be retrieved with the following commands.

- To get the list of FQDD of the RAID controllers, use **racadm storage get controllers**. The RAID controller(s) will be listed among the others.

- To get the list of FQDD of the virtual disks, run **racadm storage get vdisks** .

The following is an example from a running a system:

```
[root@cv ~]# racadm storage get controllers
RAID.SL.3-1
AHCI.Embedded.2-1
AHCI.Embedded.1-1

[root@cv ~]# racadm storage get vdisks
Disk.Virtual.239:RAID.SL.3-1
Disk.Virtual.238:RAID.SL.3-1
```

Adding the **-o** key to both of these commands will output the properties against each device which include the name and the security status. In addition, the -p option allows the user to query a specific set of properties of the devices. Check https://www.dell.com/support for further

details on the **racadm** command and its options.

Determining a vulnerable device

A system is affected if the disk encryption has been configured using the **cva disk encryption enable** command. Due to this vulnerability, the encryption is only partially configured. A system is affected if *both* of the following conditions are met.

1. Security key is assigned to the RAID controller

Run the following command:

```
racadm storage get controllers:<controller FQDD> -p SecurityStatus
```

If the output shows **SecurityStatus = Security Key Assigned,** then the security key has been assigned on the RAID controller.

Here is an example:

```
[root@cv ~]# racadm storage get controllers:RAID.SL.3-1 -p SecuritySta
tus
RAID.SL.3-1
   SecurityStatus                  = Security Key Assigned
```

However, this aforementioned output *does not mean* that the disks are indeed encrypted. To verify the disk encryption, follow step 2. Note if the above command *does not* show **Security Status = Security Key Assigned,** then the system is not affected by this issue. It means, however, that disk encryption has not been configured on this system. If the appliance supports encryption and encryption is desired, please upgrade to **CVA 6.0.7** or a later release and then run the **cva disk encryption enable** command.

2. Virtual disks are not secured

Run the following command:

```
racadm storage get vdisks --refkey <controller FQDD> -o
```

If the output shows **Secured = NO**, then the disks *are not actually encrypted*.

The following output shows the state of a system with unencrypted disks.

```
[root@cv ~]# racadm storage get vdisks --refkey RAID.SL.3-1 -o -p Secu
red
Disk.Virtual.239:RAID.SL.3-1
   Secured                          = NO
Disk.Virtual.238:RAID.SL.3-1
    Secured                          = NO
```

Indicators of Compromise

No indicators of compromise exist.

Mitigation

To manually fix the issue on a vulnerable system determined by following the steps depicted in the Determining a vulnerable device section, run the following commands to enable the encryption of the virtual disks. The FQDD of the RAID controller(s) and virtual disks will be needed for this mitigation. See the Preliminary steps section on how to retrieve them. Note as the security key was set before on this vulnerable system, it is not needed to set it again here. Please see the Caveats section for more information.

Generally, the overall process takes up to 10 minutes. The performance of a running system is not expected to degrade when the following steps are carried out.

1. Encrypt all virtual disks that belong to the RAID controller by running the following command for each of them:

```
racadm storage encryptvd:<virtual drive FQDD>
```

2. Create the job for the RAID controller and monitor its progress:

```
racadm jobqueue create <RAID controller FQDD> --realtime
```

This command must return the scheduled configuration job ID in its output. Look for **Commit JID = JID_xxxxx** in the output.
Then check the status of this job with **racadm jobqueue view -i <jobId>**. It will take up to 10 minutes to complete.

3. After the job is complete, run the following command to see if all the virtual disks are encrypted.

```
racadm storage get vdisks --refkey <RAID controller FQDD> -o
```

The output should show **Secured = YES** against each one of them.

The following is an example of the aforementioned steps.

```
[root@cv ~]# racadm storage encryptvd:Disk.Virtual.238:RAID.SL.3-1
STOR094 : The storage configuration operation is successfully complete
d
and the change is in pending state.
<--snip—->

[root@cv ~]# racadm jobqueue create RAID.SL.3-1 --realtime
RAC1024: Successfully scheduled a job.
Verify the job status using "racadm jobqueue view -i JID_xxxxx" comman
d.
Commit JID = JID_218438865303

[root@cv ~]# racadm jobqueue view -i JID_218438865303
---------------------------- JOB ------------------------
[Job ID=JID_218438865303]
Job Name=Configure: RAID.SL.3-1
Status=Running
<--snip—->
```

```
Percent Complete=[1]

[root@cv ~]# racadm jobqueue view -i JID_218438865303
--------------------------- JOB -------------------------
[Job ID=JID_218438865303]
Job Name=Configure: RAID.SL.3-1
Status=Completed
<--snip—->
Percent Complete=[100]

[root@cv ~]# racadm storage get vdisks --refkey RAID.SL.3-1 -o

Disk.Virtual.238:RAID.SL.3-1
   Status                                = Ok
   DeviceDescription                     = Virtual Disk 238 on RAID Con
troller in SL 3
   Name                                  = os
<--snip—->
   Secured                               = YES
<--snip—->

Disk.Virtual.239:RAID.SL.3-1
   Status                                = Ok
   DeviceDescription                     = Virtual Disk 239 on RAID Con
troller in SL 3
   Name                                  = data
<--snip—->
   Secured                               = YES
<--snip—->
```

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.

For more information about upgrading see CloudVision Appliance 350E-CV - Arista.

CVE-2024-7142 has been fixed in the following releases:

- CVA 6.0.7

If the user runs the **cva disk encryption enable** command in the aforementioned releases containing the fix, the disks will be properly encrypted.

In addition, the upgrade from a vulnerable CVA version to the versions mentioned above will fix the issue automatically.

- If the key/password pair is found during the upgrade, the upgrade process will encrypt the disks properly. Just to be clear, if this upgrade process *does not notice* the corresponding key/password pair on the system, it will preserve the original intent of the user and *will not* encrypt the disks.

- If the user no longer wants to encrypt the disks even though they previously ran **cva disk encryption enable** command on a vulnerable release, **cva disk encryption disable** command must be run *before the upgrade.* This **disable** option will not be available on the new releases.

Caveats

By design of the appliance, enabling the disk encryption is a one-way operation. Disabling the encryption can only be done from the RAID Controller BIOS or the iDRAC interface. In the course of disabling the encryption, all data on the disks will be wiped. A reinstallation of the CloudVision Appliance software will be necessary afterwards.

Hotfix

No hotfixes are available

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

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support