Date: October 7th, 2020

Version: 1.0

Revision	Date	Changes
1.0	October 7th, 2020	Initial Release

The CVE-ID tracking this issue is: CVE-2020-13100
CVSSv3 Base Score: 7.5/10 (CVSS:3.1/AV:N/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 eXchange (CVX) server which impacts the ControllerOob agent.

The effect of the vulnerability is that if the CVX server receives a malformed control-plane packet, the ControllerOob agent could experience a crash and subsequently restart. In such an event, all existing connections between the impacted CVX server and the managed Arista devices could flap.

Impact to production traffic is not expected as a result of such a crash. This vulnerability, if successfully exploited, would impact the control plane by limiting the CVX server's ability to manage the network or ensure that the Arista devices are updated with the latest network information. In a High Availability (HA) setup, where multiple CVX servers are running in a cluster, this vulnerability could trigger a failover of the Master Node.

Arista has not received any report of this issue being exploited in any malicious manner.

Symptoms

To confirm if this vulnerability has been hit, the following checks can be performed by logging into the CVX server.

1) Observe the following logs after running **show logging all | grep ControllerOobAgent** on the CVX server in question:

Example:

```
CVX_Node1#show logging all | grep ControllerOobAgent
ProcMgr-worker: %PROCMGR-6-PROCESS_TERMINATED: 'ControllerOobAgent' (P
ID=26962) has terminated.
ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'ControllerOobA
```

```
gent' immediately (it had PID=26962)
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'ControllerOobAgent' start
ing with PID=9195 (PPID=1736)
```

- The "%PROCMGR-6-PROCESS_TERMINATED" log highlighted above indicates that the ContrllerOobAgent has crashed. If we observe a number of these logs, each with a different Process ID (PID), it indicates that the ControllerOob agent has crashed multiple times.
- For a HA setup, please login to all three nodes and perform the same check to see if any of the nodes are exhibiting this symptom.

2) In HA setups, a failover of the Master Node (i.e. a change in the Master Node) can be observed if this vulnerability is hit. This can be verified by running **show cvx** on the CVX server:

```
CVX_Node1#show cvx
CVX Server
  Status: Enabled
  UUID: 522fc80a-d68f-11e9-82a4-a705a858a9f6
  Mode: Cluster
  Heartbeat interval: 20.0
  Heartbeat timeout: 60.0
  Cluster Status
    Name: HW-VTEP-NSX
    Role: Master
    Peer timeout: 10.0
    Last leader switchover timestamp: 5:02 ago
### Output omitted for brevity ###
```

- In the above example, the highlighted "Last leader switchover timestamp" field indicates that a new CVX server in the CVX cluster took over as the Master Node about 5 minutes ago.

3) Subsequently, we should expect to observe an agent crash log with the following output recorded by the ControllerOob agent after running **show agent logs crash** on the CVX server:

```
CVX_Node1#show agent logs crash
===> /var/log/agents/ControllerOob-23174 Tue July 23 19:17:15 2020 <==
=
===== Output from /usr/bin/ControllerOob ['--scheduled'] (PID=23174) s
tarted July 12 20:40:47.020253 ===


### Output omitted for brevity ###

rSetup: ControllerMessageEngine.tin:960: void Controller::ControllerMe
```

```
ssageSocketSm::handleReadableCount(): Assertion `cs->pbMessage()->has_
messagetype()' failed.


### Output omitted for brevity ###
```

Notes:

- **This vulnerability has been hit if and only if the output contains exactly what is highlighted in step 3.**
- For a HA setup, please login to all three nodes and perform the same check to see if any of the nodes are exhibiting this symptom.

Vulnerability Assessment

Affected Software

- CloudVision eXchange VM/Appliance:
  - 4.24.1.1F and below release in the 4.24.x train.
  - 4.23.4M and below releases in the 4.23.x train.
  - 4.22.6M and below releases in the 4.22.x train.
  - 4.21.5F to 4.21.10M releases in the 4.21.x train.

Affected Platforms

- This vulnerability affects CloudVision eXchange software running on virtual and physical appliances in the versions identified above.
- The following products are **not affected:**
  - EOS running on Arista switching platforms (CVX clients)
  - Arista Wireless Access Points
  - CloudVision Wi-Fi, virtual appliance or physical appliance
  - CloudVision Wi-Fi cloud service delivery
  - CloudVision Portal, virtual appliance or physical appliance
  - CloudVision as-a-Service
  - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
  - CloudEOS Container, that runs in Kubernetes on-premises clusters
  - Arista 7130 Systems running MOS
  - Arista CCF (Converged Cloud Fabric) and DMF (DANZ Monitoring Fabric) (formerly Big Switch BCF and BMF)

Mitigation

To limit the ability of untrusted devices to affect the CVX server, Control-Plane Access-Control Lists (CP ACLs) can be used to limit connections to known CVX clients only. CVX uses TCP ports 50003 and 50004 for communication on the CVX server.

For the final resolution, please refer to the next section which lists the details of the hotfix and remediated software versions.

Resolution

This vulnerability is being tracked by Bug 483850. To safeguard against this vulnerability, the recommended course of action is to install the provided hotfix or to perform an upgrade to a remediated EOS version.

The vulnerability has been fixed in the following EOS versions:

- 4.24.2F
- 4.23.5M
- 4.22.7M
- 4.21.12M

The hotfix has been implemented as an extension, which can be downloaded from the following link:

https://www.arista.com/assets/data/SecurityAdvisories/SA52/SecurityAdvisory0052Hotfix.swix

Sha512sum: cd0333153a3d8e78df75975de056dd896d4dab89013fa21755742a28af677ef1c7280f829ca3a4c06b6788cd4f60e21dca982d9a89062cc0bf986fe2709a1ab7 SecurityAdvisory0052Hotfix.swix

For instructions on the installation and verification of extensions, please refer to the following section in the EOS User Manual:

https://www.arista.com/en/um-eos/eos-section-6-7-managing-eos-extensions

The extension will need to be made persistent across reboots by copying the installed-extensions to boot-extensions.

Note:

After the installation of the hotfix, it is expected for the CVX agents (ex. ControllerOoB) to restart. Impact to production traffic is not expected as a result of these restarts. As a best practice, it is recommended to install the hotfix during a maintenance window or during non-production hours.

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