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-2020-13881
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Description

This advisory documents the impact of a vulnerability in an external TACACS+ server library used by Arista's CloudVision Portal. This vulnerability only impacts systems configured with TACACS+ authentication for the base operating system, which is configured via the cvpadmin shell. The effect of this vulnerability is that the TACACS+ encryption key, used for communication to the TACACS+ server, is logged by journald. While user passwords are not logged, this vulnerability exposes the secret key for CloudVision Portal to TACACS+ communication. An attacker who is able to capture traffic between the CloudVision Portal instance and TACACS+ would then be able to decrypt the traffic and read all information passed to and from the TACACS+ server. This traffic may include user passwords. This vulnerability only concerns SSH logins to the CloudVision Portal, and not for Web UI logins. Users who only access CloudVision Portal via the Web UI are not at risk.

Bug 485085 tracks this vulnerability. This is an internally found vulnerability and there has been no report of exploitation in the field.

Symptoms

This is a passive attack, as detailed above, and does not manifest into any observable symptom. Here are the steps to determine if TACACS+ is enabled/configured for the base operating system, which is configured via the cvpadmin shell.

/cvpi/cvp-config.yaml

```
[root@cvp-2020-2-0-ga ~]# cat /cvpi/cvp-config.yaml | grep tacacs -A2
  tacacs:
    ip_address: 10.83.12.22
    key: arista
```

/etc/pam.d/sshd

```
[root@cvp-2020-2-0-ga ~]# cat /etc/pam.d/sshd | grep tacacs
auth       include      tacacs
auth       include      tacacs
```

Vulnerability Assessment

Affected Software

CloudVision Portal
All releases prior to 2020.1.2

For releases prior to CVP 2020.1.2, if an attacker has access to the journald logs of CVP, a MITM (Man-In-The-Middle) attack could be carried out to get the username and password of CloudVision Portal VM CLI users that are authenticated via TACACS+.

Affected Platforms

- This vulnerability affects CloudVision virtual and physical appliances 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)

Resolution

The vulnerability is 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. Once upgraded, the encryption key will no longer be logged by journald. To protect against the risks from the key being logged prior to the upgrade, it is recommended to change the password for both the TACACS+ and Administrator passwords after the upgrade.

This CVE is not applicable if TACACS+ authentication is not set up for the base VM login for CloudVision Portal (i.e. exposure is applicable to the CVP shell, and not the web UI).

Vulnerability References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13881
- https://github.com/kravietz/pam_tacplus/issues/149

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