Date: December 4th, 2019

Version: 1.0

Revision	Date	Changes
1.0	December 4, 2019	Initial Release

CVE-ID tracking this issue is: CVE-2019-18615
CVSSv3 Base Score: 7.4 (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N)

Description:

This advisory documents the impact of an internally found security vulnerability for CloudVision Portal (CVP) where, under certain conditions, the application logs user passwords in plain text for certain API calls, potentially leading to user password exposure. This only affects CVP environments where:

- Devices have enable mode passwords which are different from the user's login password, OR
- There are configlet builders that use the Device class and specify username and password explicitly

Application logs are not accessible or visible from the CVP GUI. Application logs can only be read by authorized users with privileged access to the VM hosting the CVP application.

Bugs tracking this vulnerability are 415120, 423105

Affected Software Versions:

CloudVision Portal
All releases in the 2018.2 Train

Resolution:

This vulnerability is addressed in the 2019.1.0 and later versions of CloudVision Portal. We recommend upgrading to a remediated release to safeguard against this vulnerability.

This vulnerability has limited exposure based on the conditions listed in the description. As security best practices, it is recommended to restrict access to the CVP host operating system to trusted users/user groups and periodically rotate user passwords.

Vulnerability References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18615

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