Date: December 4th, 2019

Version: 1.0

Revision	Date	Changes
1.0	December 4, 2019	Initial Release

The CVE-ID tracking this issue is: CVE-2019-18181

CVSSv3 Base Score: 5.6 (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N)

Description:

This advisory documents the impact of an internally found privilege escalation vulnerability where CloudVision Portal allows users with read-only permissions to bypass permissions for restricted functionality via CVP API calls through the Configlet Builder modules. This vulnerability can potentially enable authenticated users with read-only access to take actions that are otherwise restricted in the GUI. Bug 425371 tracks this vulnerability.

Affected Software Versions:

CloudVision Portal
All releases in the 2018.1 Code train
All releases in the 2018.2 Code train

For releases in the 2018.1 code train, the vulnerability allows unauthorized users to have read and write access for certain paths of the filesystem, whereas in the 2018.2 code train, the unauthorized user's access is restricted to read-only.

Resolution:

The 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.

Additionally, for the 2018.2 release train, a hotfix is available in the form of a python script that updates permissions for the affected APIs. For the 2018.1 code train, the suggested course of action is to upgrade to one of the remediated release versions (2019.1.0 and above).

Patch file download URL: SecAdvisory0044Hotfix.pyc

Sha512sum checksum for verification:
683eccf4ea8774d8d29d91c2aab5ceb18d9b41704d42350fa43ae8d8b72955d9054017ac0bbc887840b034df69116299d0230fc0c33e41c2422a9c019e2bb70d

Steps to run/validate the script:

1. ESSH as a privileged user to the VM hosting the CVP application
2. Create a directory for security patches using this command -

```
mkdir -p /cvpi/SecurityPatches/logs
```

3. Copy the hotfix script to the above path and install the patch by running command

```
python SecAdvisory0044Hotfix.pyc
```

4. On successful install the following message will be displayed:

```
Hotfix is applied successfully
```

5. Logs are also stored in “/cvpi/SecurityPatches/logs” directory

Vulnerability References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18181

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