

**Date:** December 1st, 2016

**Version:** 1.1

Revision	Date	Changes
1.0	December 1st, 2016	Initial Release
1.1	December 6th, 2016	Impact section of this advisory is updated

**Affected Platforms:** CloudVision Portal (CVP) only.

**Affected Software Version:** All CloudVision Portal versions before 2016.1.2.1

**The CVE-ID tracking this issue is CVE-2016-9012**

**CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)**

**CVSS v3 Base Score: 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)**

**Impact:** This vulnerability allows a potential attacker with access to the management plane to gain access to the internal configuration mechanisms of CVP and take over the CVP instance.

**NOTE:** This vulnerability was identified internally by Arista Networks and Arista has not received evidence of this being exploited, as of the date of this update.

**BUG174047** tracks this vulnerability. A fix for this issue is available in 2016.1.2.1.

The following log message in the access.log file in /var/log/nginx indicates that this vulnerability was exploited to gain access to the CVP system

```
[user@cvp15 nginx]# grep "system/console/bundles" access.log
```

```
"GET /web/system/console/bundle HTTP/1.1" 401 0 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36" "-"
```

**Resolution:** It is strongly recommended to upgrade all CloudVision Portal cluster members to version 2016.1.2.1 to address this vulnerability. Please follow the upgrade procedure provided in the [CloudVision configuration guide](#) for 2016.1.2.1

Please note that CVP fast upgrade is supported only from 2016.1 (or later) to 2016.1.2.1.

## References:

CVE-2016-9012

Open a Service Request:  
By email: [support@arista.com](mailto:support@arista.com)  
By telephone: 408-547-5502  
866-476-0000