Date: May 15th, 2017

Version: 1.0

Revision	Date	Changes
1.0	May 15th, 2017	Initial Release

Arista Products vulnerability report for CVE-2016-7117

On October 2016, information was released about a security advisory for a vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2

From internal investigations it has been confirmed that Arista Network's software products EOS and Cloud Vision Portal (CVP) are not exploitable to this vulnerability.

Description:

Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.

This security issue relies on the user being able to have precise control over how the system call is invoked to trigger any potential issues, making this a non-issue within Arista products. However we have opened BUG186359 and BUG188078 to address this scenario in future EOS and CVP releases respectively.

References:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7117
http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.2

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