Date: May 14th 2015

Revision	Date	Changes
1.0	May 14th, 2015	Initial release
1.1	November 22nd, 2017	Resolution section updated to reflect the correct BUGID

Arista 7000 Series Products and Arista EOS are vulnerable to CVE-2015-3456.

On May 13th, 2015 information was released about a buffer overflow vulnerability affecting the Floppy Disk Controller emulation in the QEMU component of the KVM/QEMU which has been assigned CVE-2015-3456 and commonly referred to as VENOM. A privileged guest user could use this flaw to potentially execute arbitrary code on the host of the VM, the host being the switch in this case.

All shipping releases of Arista EOS have a feature to host guest virtual machines. This feature uses the QEMU component in the Linux kernel which makes EOS vulnerable if all of the following conditions are present:

- A virtual machine is configured and is running on EOS
- Untrusted users are allowed access to the virtual machine hosted on EOS
- Untrusted users that don't have access to the network devices but have access to the virtual machine hosted by EOS

The list of virtual machines hosted by EOS can be viewed by running the command 'show virtual-machines':

```
switch(config)#show virtual-machine
VM Name              Enabled    State
-------              -------    -----
foo                  Yes        Running
```

Mitigation:

Arista recommends securing access to the virtual machines running on EOS by granting privileged guest access to trusted users only.

Resolution:

Copyright 2024 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Bug 119467 tracks this vulnerability. The fix will be available in EOS releases 4.15.2F, 4.14.8M, 4.13.13M, 4.12.11M and 4.11.12M

References:
For additional information about the vulnerability, please visit:
https://access.redhat.com/articles/1444903

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

Copyright 2024 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.