Date: September 23rd, 2015

Revision	Date	Changes
1.0	September 23rd, 2015	Initial release
1.1	August 11th, 2023	Updated discovered EOS version (4.12.1)

Arista Products vulnerability report for security released for QEMU between August 27th and September 15th, 2015

The Fedora project issued a series of vulnerabilities for QEMU that affect the Arista family of products and EOS.

QEMU is a generic and open source machine emulator used natively in Fedora based systems. All shipping releases of Arista EOS have a feature to host guest virtual machines. This feature uses the QEMU process 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 although they may not have access to the EOS CLI.

The list of virtual machines hosted by EOS can be viewed by running the command ‘show virtual-machines’. The vulnerability is applicable only to the QEMU component and hence only switches hosting VMs in EOS are affected.

This advisory documents the vulnerability status of Arista 7000 Products and Arista EOS in response to the vulnerabilities listed below:

CVE-2015-5239 Qemu: VNC display driver in Qemu is vulnerable to an infinite loop issue

Vulnerability Status:	Affected
Details:	An integer overflow issue was found in the VNC display driver of the QEMU emulator, which could be used by a privileged guest user to create a denial of service attack. The integer overflow led to an infinite loop inside the VNC driver, eventually crashing the QEMU process on the switch.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch

Solution:	Bug 132460 tracks this issue. Issue was discovered in version 4.12.1. Upgrading to software versions 4.12.2 and newer will resolve the issue.

CVE-2015-5278 (qemu: net: avoid infinite loop when receiving packets)

Vulnerability Status:	Affected
Details:	A flaw was found where a QEMU emulator built with NE2000 NIC emulation support was vulnerable to an infinite loop issue that occurred when receiving packets over the network. A privileged user inside a guest (VM) could use this flaw to crash the QEMU instance, resulting in a denial of service for QEMU users.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 132492 tracks this issue. Issue was discovered in version 4.12.1. Upgrading to software versions 4.12.2 and newer will resolve the issue.

CVE-2015-5279 (qemu: Heap overflow vulnerability in ne2000_receive() function)

Vulnerability Status:	Affected
Details	A flaw was found where a QEMU emulator built with NE2000 NIC emulation support was vulnerable to a heap buffer overflow issue that occurred when receiving packets over the network. A privileged user inside a guest (VM) could use this flaw to crash the QEMU instance (denial of service) or potentially execute arbitrary code on the switch.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 132493 tracks this issue. Issue was discovered in version 4.12.1. Upgrading to software versions 4.12.2 and newer will resolve the issue.

CVE-2015-6815 (qemu: net: e1000 infinite loop issue)

Vulnerability Status:	Affected
Details	A flaw was found in the way a QEMU-emulated e1000 network interface card processed transmit descriptor data when sending a network packet. A privileged guest user could use this flaw to crash the guest (VM on switch)
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 132494 tracks this issue. Issue was discovered in version 4.12.1. Upgrading to software versions 4.12.2 and newer will resolve the issue.

CVE-2015-6855 (qemu: ide: divide by zero issue)

Vulnerability Status:	Affected
Details:	It has been discovered that a QEMU emulator built with IDE disk and CD/DVD-ROM emulation support is vulnerable to a divide-by-zero issue. A privileged user inside the guest could use this flaw to crash the QEMU instance, resulting in a denial of service for QEMU users.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 132496 tracks this issue. Issue was discovered in version 4.12.1. Upgrading to software versions 4.12.2 and newer will resolve the issue.

References:
For additional information about the vulnerability, please visit:

- CVE-2015-5239
- CVE-2015-5278
- CVE-2015-5279
- CVE-2015-6815
- CVE-2015-6855

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