Date: September 4th 2015

Revision	Date	Changes
1.0	September 4th, 2015	Initial release

Arista Products vulnerability report for security updates released for QEMU on August 23rd, 2015.

In August 2015 the Fedora project issued an update for QEMU that addresses a list of vulnerabilities

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
- 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'

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

CVE-2015-5166 (qemu: BlockBackend object use after free issue)

Vulnerability Status:	Not Affected
Details:	Vulnerability is specific to the Xen hypervisor which does not ship in EOS

CVE-2015-5745 (qemu: buffer overflow in virtio-serial)

Vulnerability Status:	Affected
Details:	A user logged on to the guest OS can cause QEMU to crash
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch

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.

Solution:	Bug 131404 tracks this issue and the fix will be available in the next release of the currently supported EOS releases - 4.15, 4.14, 4.13 and 4.12

CVE-2015-3209 (qemu: pcnet: multi-tmd buffer)

Vulnerability Status:	Affected
Details	Heap based overflow in QEMU allows remote attackers to execute arbitrary code on the host.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 131402 tracks this issue and the fix will be available in the next release of the currently supported EOS releases - 4.15, 4.14, 4.13 and 4.12

CVE-2015-5165 (qemu: rtl8139 uninitialized heap)

Vulnerability Status:	Affected
Details	The user on the guest virtual machine could read uninitialized qemu memory on the switch and run arbitrary code
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 131406 tracks this issue and the fix will be available in the next release of the currently supported EOS releases - 4.15, 4.14, 4.13 and 4.12

CVE-2015-5154 (qemu: ide: atapi: heap overflow during I/O buffer memory access)

Vulnerability Status:	Not Affected
Details:	EOS only supports using an ISO image as a disk image. This vulnerability is exploited only when the container has a CD-ROM drive enabled.

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.

CVE-2015-3214 (qemu/kvm: i8254: out-of-bounds memory access in pit_ioport_read function)

Vulnerability Status:	Affected
Details:	QEMU before 2.3.1 does not distinguish between read lengths and write lengths, which might allow users on the guest VM to execute arbitrary code on the switch by triggering use of an invalid index.
Mitigation:	Ensure only trusted users have access to the guest VMs hosted on the switch
Solution:	Bug 131493 tracks this issue and the fix will be available in the next release of the currently supported EOS releases - 4.15, 4.14, 4.13 and 4.12

References:
For additional information about the vulnerability, please visit:
https://lists.fedoraproject.org/pipermail/package-announce/2015-August/164489.html

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.