VULNERABILITY SUMMARY

On May 13, 2015, a vulnerability was disclosed in the QEMU Floppy Drive Controller that, when exploited, could allow an attacker to escape a virtual machine on certain open source hypervisors. CVE-2015-3456 (VENOM) has been assigned for this vulnerability; details can be found at the link below:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3456

WHAT IS THE IMPACT TO FIREEYE PRODUCTS AND SERVICES?

FireEye's hypervisor is among many technologies that leverage the open source component that was publicly disclosed today as having a critical vulnerability (CVE-2015-3456). FireEye employs many measures in its products to limit the impact of these types of issues through secure development practices and operational processes that ensure we respond quickly to security issues. Because of this, we can – and have – responded to VENOM by ensuring immediate availability of patches to customers for all of our major products.

FireEye was notified through the coordinated disclosure efforts of the open source and security research communities. We are unaware of any active exploits against this vulnerability; however, FireEye urges its customers to upgrade their affected appliances as soon as possible to ensure fidelity of their FireEye products and continued protection of their organization.

We have published a detailed customer support notice and made it available through our customer support channels. This publication includes details on specific products, dates for remediation (if required), and mitigating actions (if necessary). FireEye will update the customer support notice as more information becomes available. As always, FireEye recommends following the best practices below to limit exposure in the case of a vulnerability such as VENOM.

BEST PRACTICES

FireEye recommends that customers implement the following best practices when possible. These practices will help protect customers between the times when new vulnerabilities are discovered and customers are able to install new patches.

- Always keep the product version up-to-date.
- Limit network access to and from appliance management interfaces with firewalls (or other protective measures).

- Only issue accounts to trusted administrators.
- Utilize strong passwords.
- Restrict physical access to the appliance to trusted administrators.

FireEye, Inc., 1440 McCarthy Blvd., Milpitas, CA 95035 | +1 408.321.6300 | +1 877.FIREEYE (347.3393) | info@FireEye.com | www.FireEye.com 1

Notes

This advisory will be updated as patch status changes, or as other information becomes available.

Revision history:

- May 13, 2015 – Initial version

For product- and service-specific information, please visit the FireEye Customer Support Portal.

https://www.fireeye.com/support/contacts.html

To report vulnerabilities in FireEye products, please email Security[at]FireEye.com or visit https://www.fireeye.com/security