Revised January 30, 2015 FireEye Security Notice

Statement About GHOST Vulnerability: CVE 2015-0235

Summary

On January 27, 2015, a publicly disclosed vulnerability was revealed in the Linux glibc library that allows an attacker to conduct remote code execution to gain complete control of a compromised system. A patch is available for affected Linux versions and operating systems. CVE-2015-0235 has been assigned for this vulnerability; details can be found at the below link:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235

What Is The Impact To FireEye Products and Services?

FireEye is in the process of evaluating the GHOST vulnerability's impact to all products and services within our portfolio. **When FireEye has additional details and updates, they will be available for customers directly through customer support channels.** This update will include details on specific products, dates for remediation (if required), and mitigating actions (if necessary). FireEye will continue to update this notice periodically as necessary or if more information becomes available. As always, FireEye recommends following the below general best practices to limit exposure in the case of a vulnerability such as GHOST.

Best Practices

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

- Always keep the product version up-to-date.
- Limit network access to appliance management interface(s) and ports with firewalls (or other protective measures).
- Only issue accounts to trusted administrators.
- Utilize strong passwords.
- Restrict physical access to the appliance to trusted administrators.

Notes

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

Revision history:

- January 27, 2015 – Initial version
- January 30, 2015 – Updated with link to FireEye Customer Support Portal

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 http://www.fireeye.com/security.