Vulnerability Summary

September 8th, 2015

On Monday, September 7, 2015 FireEye learned of four potential security issues in our products from Kristian Hermansen's public disclosure. We have reached out to Mr. Hermansen to get more details on the reported "file disclosure" issue, as well as claims about remaining vulnerabilities, and will work with him to address them.

Upon initial review of the limited information available in today's public disclosure, we have found that the "file disclosure" issue from Mr. Hermansen impacts a legacy version of the FireEye endpoint platform (referred to as "HX"). Recent updates have reduced the impact of this issue to customers running legacy versions of the product (HX 2.1.x and DMZ 2.1.x). However, in order to eliminate risk immediately, FireEye strongly recommends **upgrading to the current release (version 2.6.x) of the HX product.**

For customers who remain on the legacy version, FireEye is actively working on a fix for the reported issue in the HX 2.1.x series and will update impacted customers through our official Customer Support channels.

In addition to the recommendations above, we also encourage all FireEye customers to leverage the security best practices (provided below) where possible in their environments to continue to limit security risk exposure.

We'd like to emphasize that we appreciate the efforts of security researchers and always encourage responsible disclosure of security issues per our policy on the http://www.fireeye.com/security website.

FireEye Security Best Practices

FireEye recommends that the following steps be taken to protect the listed FireEye products:

- Always keep the product version up-to-date
- Limit network access to the management interface(s) of the appliance with firewalls or similar measures
- Only issue accounts to trusted administrators
- Utilize strong passwords
- Monitor logs
- Restrict physical access to the appliance to trusted administrators

Revision history:
_____ – Initial version

For further information, contact FireEye Customer Support.

http://www.fireeye.com/support/contact-customer-support.html

To report vulnerabilities in FireEye products, please send an email to security[at]FireEye.com.