Q4 Security Advisory

December 31, 2015

Executive Summary

FireEye has issued a set of FireEye Operating System (FEOS) updates for the following products: NX, EX, AX, FX, HX and CM. FireEye also continuously issues security updates to our operational infrastructure and applications. These updates contain a number of vulnerability fixes credited to researchers other than FireEye.

Recommendations

FireEye encourages all customers to update their systems to the latest released version where noted below. FireEye has issued maintenance releases and fixes for all security issues contained within this advisory.

Fixed Versions

The following FEOS versions (and later, except where noted) contain fixes for the security issues listed in this advisory:

- NX 7.6.1 released 10/15/2015
- EX 7.6.2 released 10/15/2015
- AX 7.7.0 released 10/05/2015
- FX 7.5.1 released 10/05/2015
- CM 7.6.2 released 10/15/2015
- HX 2.1.8 released 12/15/2015
- HXD 2.2.2 released 12/15/2015

Summary of Security Issues

- Analysis Engine Evasion
- FireEye Website Input Validation on Email Form
- URL-Encoded Text Injection
- HX Input Validation on Backup Engine
- HX Login Page Display Output Error
- HX Input Validation on Configuration Page

FireEye Label: Analysis Engine Evasion
Credit: Moritz Jodeit, Blue Frost Security GmbH
Severity: High
Products Affected: FX, AX, NX, EX
Description: An evasion existed that would allow files to bypass the FireEye detection engine. The issue has been addressed.
Version and Fix Details:

Product	Fixed FEOS Version	Date Released	Customer Actions Required
FX	7.5.1	10/05/2015	Update to the latest version
AX	7.7.0	10/05/2015	Update to the latest version
NX	7.6.1	10/15/2015	Update to the latest version
EX	7.6.2	10/15/2015	Update to the latest version

FireEye Label: FireEye Website Input Validation on Email Form
Credit: Roy Jansen
Severity: Low
Products Affected: FireEye website
Description: A vulnerability existed within our website allowing un-sanitized email form field input which could have led to an attacker to pass malicious content masquerading as a FireEye email.
Version and Fix Details:

Service	Version Released	Date Released	User Actions Required
FireEye Website	Current	11/05/2015	None

FireEye Label: URL-Encoded Text Injection
Credit: Oded Vanunu and Avi Gimpel
Severity: Low
Products Affected: FX, AX, NX, EX, CM
Description: A specially crafted URL could allow plain text to be rendered on the FireEye Web User Interface post-authentication.
Version and Fix Details:

Product	Fixed FEOS Version	Date Released	Customer Actions Required
FX	7.5.0	09/15/2014	Update to the latest version
AX	7.7.0	10/05/2015	Update to the latest version
NX	7.5.0	01/22/2015	Update to the latest version
EX	7.6.0	07/07/2015	Update to the latest version
CM	7.5.0	01/22/2015	Update to the latest version

FireEye Label: HX Input Validation on Backup Engine
Credit: Pondurance LLC and Pondurance LLC security engineer, Curtis Brazzell
Severity: Medium
Products Affected: HX, HXD **
Description: A post-authentication security vulnerability existed that could have allowed an attacker to pass un-sanitized input to the HX backup/restore engine causing local code execution.
Version and Fix Details:

Product	Fixed FEOS Version	Date Released	Customer Actions Required
HX	2.1.7	09/28/2015	Update to the latest version
HXD	2.2.1	09/28/2015	Update to the latest version

FireEye Label: HX Login Page Display Output Error
Credit: Pondurance LLC and Pondurance LLC security engineer, Curtis Brazzell
Severity: Low
Products Affected: HX, HXD **
Description: A minor error where system command output was incorrectly displayed to the user has been fixed.
Version and Fix Details:

Product	Fixed FEOS Version	Date Released	Customer Actions Required
HX	2.1.7	09/28/2015	Update to the latest version
HXD	2.2.1	09/28/2015	Update to the latest version

FireEye Label: HX Input Validation on Configuration Page
Credit: Pondurance LLC and Pondurance LLC security engineer, Curtis Brazzell
Severity: Medium
Products Affected: HX, HXD **
Description: A lack of input validation in a configuration page existed that could have allowed an authenticated user to execute arbitrary commands.
Version and Fix Details:

Product	Fixed FEOS Version	Date Released	Customer Actions Required
HX	2.1.8	12/15/2015	Update to the latest version
HXD	2.2.2	12/15/2015	Update to the latest version

**** Special Advisory Note on HX**
Recent updates have reduced the impact of this issue to customers running older versions of the product (HX/HXD 2.1.x and 2.2.x). However, in order to eliminate risk immediately, FireEye strongly recommends upgrading to the current release (version 3.0.1) of the HX product.

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

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 and maintain default automated Security Content update configuration setting**
- 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

If you have any questions, please contact FireEye Support at support@fireeye.com or 877 347-3393 (877-FIREEYE) or 408 321-6300.

To report security issues in FireEye products, infrastructure, or services, please send an email to security[at]FireEye.com.