FireEye

Security Bulletin

Revised July 8, 2014 FireEye Security Bulletin #001

Security Vulnerability Roll-Up Notice

Summary

FireEye has issued a set of FireEye Operating System (FEOS) updates for the following products: NX, EX, AX, FX, and CM. These updates contain a number of vulnerability fixes, some of which are listed in detail in this document. Many of these fixes have previously been communicated in product release notes. This bulletin denotes the first formal, separate FireEye security bulletin for this product family so that our customers and other interested parties can now track and maintain security vulnerability information. We intend to have future bulletins contain a comprehensive list of security fixes since the previous release. These releases underwent a set of external security reviews, and a targeted security redesign by FireEye development. These releases bring the listed products to the same security parity.

Recommendation:

FireEye encourages all customers to upgrade to the most current releases as soon as practical - especially customers running versions older than 7.1.0. As always, FireEye recommends that customers keep up with current releases for both fixes as well as functionality improvements. We also recommend that customers follow certain best practices, noted later in this document.

Fixed Versions

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

- NX 7.1.1.222846 released Jun 12, 2014
- EX 7.1.1.222846 released Jun 12, 2014
- AX 7.1.0.223064 released Jun 12, 2014
- FX 7.1.0.224362 released Jun 30, 2014
- CM 7.1.1.222846* released Jun 12, 2014

* Exception: Special version CM 7.1.2 does not have all fixes. Customers using CM 7.1.2 should upgrade to 7.2.0 or above, which includes all fixes.

Note: The FEOS release is displayed within the Web UI footer or can be obtained by the '**show ver**' CLI command.

Vulnerabilities

The following vulnerabilities were fixed as of the versions listed above:

Multiple OpenSSL Vulnerabilities - CVE-2010-5298, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, and CVE-2014-3470

Severity: Important

The OpenSSL Project has identified five vulnerabilities (affecting the FireEye platform) that may allow man-in-the-middle (MITM) attackers to read from, or inject information into, an encrypted stream, remotely execute arbitrary code on the server, or cause a denial of service. The OpenSSL advisory can be found at:

https://www.openssl.org/news/secadv_20140605.txt.

Note: Based on an internal evaluation by FireEye of the vulnerabilities and how we make use of the OpenSSL library, we believe these products were only vulnerable to CVE-2014-0224, the active MITM crypto downgrade attack. However, we have implemented the fixes for the others as a preventative measure.

FEOS CLI Command Injection Vulnerability – (No CVE number assigned)

Severity: Important

FireEye has fixed a post-authentication command injection vulnerability in the command-line interface of the affected products. An attacker could issue a special sequence of commands that would allow them to execute arbitrary shell commands in the underlying operating system of the appliance. To take advantage of this vulnerability, an attacker must be able to communicate with the SSH management interface of the appliance AND have valid login credentials, or the attacker must have physical access to the console interfaces of the appliance.

- FireEye would like to thank Silent Signal for reporting this vulnerability to us and working with us while we prepared a fix.

FireEye Multiple Vulnerabilities – (No CVE numbers assigned)

Aggregate Severity : Critical

In the 7.1 release for the affected products, FireEye contracted with an independent external vulnerability assessment firm to evaluate the security of our products. We then invested a significant amount of time and resources to systemically audit and remediate several classes of vulnerabilities discovered across the code base. These vulnerabilities ranged in severity from Low to Critical. The most severe of these vulnerabilities would allow an unauthenticated remote attacker to inject shell commands into the FEOS as the root user. In all cases, to take advantage of any of the vulnerabilities, an attacker would have to be able to communicate with the management interface of the products.

Security fixes and enhancements were made in the following areas:

- Web UI command injection
- Web UI SQL injection
- Processes executing with higher than necessary privileges
- Cross-site scripting
- Cross-site request forgery
- Web UI file system read and write vulnerabilities
- Updated insecure third-party libraries
- Internal services unnecessarily exposed via TCP/IP

FireEye is not aware of any instances of these vulnerabilities being exploited in the wild.

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
- Restrict physical access to the appliance to trusted administrators

If you have any questions, or if you would like the updated FEOS releases noted above, please contact FireEye Support at support[at]FireEye.com or 877 347-3393 (877-FIREEYE) or 408 321-6300.

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