FireEye Notice: Disclosed Vulnerabilities

July 9, 2014

On July 7, 2014, FireEye responded to a public disclosure of some suspected security issues in the FireEye AX product line by a researcher, Jean-Marie Bourbon. As a major participant and contributor in the security community, FireEye continues to be an avid supporter of security research and strongly encourages responsible and safe disclosure of FireEye product vulnerabilities. FireEye takes product security vulnerabilities very seriously and actively encourages, supports, and responds to any product security issue or concern that is formally reported to FireEye. In fact, many of our customers have helped to strengthen the security posture of our product family over time based on their feedback and reporting.

While this particular disclosure was outside of the standard procedures for reporting these types of vulnerability issues, FireEye is appreciative of the items reported by Bourbon. FireEye has provided this analysis in response to those issues raised in order to reassure our customers and the research community that we are actively engaged and will always be an advocate for transparency and responsible reporting of any product vulnerability. We have concluded that the net vulnerability impact to our customers in this case is low to moderate. An update will be available to address these issues in the next product software release. Details of the findings are included in this bulletin.

Eight issues were identified as potential vulnerabilities reported by Bourbon. FireEye has evaluated each issue against the current versions of our FireEye Operating System (FEOS), as well as the older version of the product that was evaluated by Bourbon.

For the eight items, we have determined:

- Two were duplicates in the same report
- Two of them are not vulnerabilities (no security problem exists)
- Two of them did exist in FEOS 6.4, but were already fixed in 7.1.0, which was released before we became aware of this report
- Two of them still exist in current versions of some products, and are rated low to moderate

As part of our standard release process, FireEye products were independently evaluated and a number of third-party vulnerability assessments were completed as well as in-house testing. The findings from those tests were remediated in the 7.1.x release of FEOS including many of the referenced vulnerabilities in this notice. The vulnerabilities affected the following products: NX, EX, CM, AX, and FX.

FireEye recommends that **all customers upgrade to the current release for the NX, EX, CM, AX, and FX products as soon as practical**.

A separate FireEye security bulletin covering this release was already in progress when the disclosure occurred, and is available here:

http://www.fireeye.com/resources/pdfs/support-notices/security-bulletin-001.pdf

As a standard practice for protecting our customers, FireEye does not publicly acknowledge vulnerabilities or security issues until a fix has been released for the affected products. There may be exceptions that occur from time to time if circumstances dictate, as is the case with this notice. When these exceptions arise, FireEye will release information so that a customer (or other affected user) can determine the best course of action to mitigate risk in their environment. This may include recommendations for mitigating controls and will not include or reference specific information to enable exploitation of the vulnerability. Following this practice and based on our analysis of the situation, FireEye is providing details of the findings below (assessed as low to moderate severity) as well as options for mitigation.

FireEye Multiple Vulnerabilities – (No CVE numbers assigned)

Aggregate Severity: Moderate
Summary: Out of the eight issues listed, four of them were actual vulnerabilities. As of the 7.1.0 release, two are fixed, and two remain in current versions. The two remaining are one Low severity XSS, and one Moderate severity information disclosure vulnerability. These two vulnerabilities will be fixed in a future release.

Note: All of the claimed vulnerabilities whether accurate or not would only be exploitable post-authentication, and require direct network access to the management interfaces of the appliances.

Three XSS vulnerabilities
Severity: Low
Products affected: NX, EX, CM, AX, FX

The report lists three XSS vulnerabilities. These vulnerabilities did exist in the 6.4.1 FEOS version. Two of them were fixed in 7.1.0 and one of them still exists in currently released versions. We will be releasing a fix for the remaining XSS vulnerability in a future FEOS release. The vulnerability requires that the victim first be logged into the Web interface of the affected appliance.

CSRF vulnerability
Severity: Low
Products affected: NX, EX, CM, AX, FX

The report lists a CSRF vulnerability. This vulnerability did exist in the 6.4.1 FEOS version. It was fixed in 7.1.0. FireEye does not believe that this vulnerability qualifies as a true CSRF, and is a duplicate of one of the fixed XSS vulnerabilities. For the listed variant, the user would have to be directed to the appropriate page AND manually click on a particular button to take the action, making exploitation unlikely. The vulnerability requires that the victim first be logged into the Web interface of the affected appliance.

SQL injection
Severity: N/A
Products affected: N/A

The report lists a SQL injection vulnerability. FireEye has evaluated the claim, and determined that this vulnerability does not exist. The SQL query is parameterized, and the error message indicates as much. The report also lists a potential JSON variant FireEye considers a duplicate issue, and is not vulnerable for the same reason.

Filesystem information disclosure
Severity: Moderate
Products affected: AX, FX

The report lists a file and directory disclosure vulnerability. This vulnerability did exist in the 6.4.1 FEOS version and still exists in the currently shipping versions of AX and FX. We will be releasing a fix for this vulnerability in a future FEOS release. To take advantage of this vulnerability, an attacker must possess administrative (trusted) credentials and alter the system configuration. Given that possession of an admin account and access to the administrative interface of the appliance would permit an attacker to perform much more serious actions, we do not believe this vulnerability poses any serious threat to our customers. In addition, changes to system configurations are logged and should be monitored as a security best practice.

“Source code info-leak”
Severity: N/A
Products affected: N/A

The report also contained a “source code info-leak” vulnerability report. FireEye has evaluated this report and determined that this is simply a duplicate of one of the already mentioned XSS vulnerability, the one that is still present. The code that is displayed using the sample contained in the report is client-side HTML code, the same code one could see by using the browser’s view source function.

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:
July 9, 2014 – 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 email security[at]FireEye.com.