Vulnerability Summary

September 8, 2015

FireEye was informed of five security issues in the FireEye Operating System. FireEye had already identified two of the five issues and three were new findings credited to research firm ERNW. FireEye has issued maintenance releases for customers resolving all five vulnerabilities.

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

FireEye customers will also receive specific version information on maintenance releases and other customer-specific details in a separate bulletin delivered directly through our Customer Support channels.

FireEye Label: *Command Injection in Management Web Interface - Post Authentication (1 of 5)*
Severity: Low
Products affected: NX, EX, CM, AX, FX
Credit: N/A

A vulnerability existed that would allow an authenticated user with full administrative privileges, and access to the management interface, to gain full access to the underlying system. Given that possession of an administrative account and access to the administrative interface of the appliance would permit an attacker to perform much more serious actions, we have concluded in our analysis that this vulnerability poses a minimal threat to our customers.

FireEye Label: *MVX Traffic Analysis Buffer Overflow (2,3 of 5)*
ERNW Paper: Memory Corruption Vulnerabilities (Section 3.1)
Severity: Moderate
Products affected: NX, EX, AX, FX
Credit: Felix Wilhelm of ERNW

A buffer overflow vulnerability present in code involved with analyzing malware samples that could allow an attacker to cause a limited denial of service. (This vulnerability accounts for two out of the five identified in the same component that was patched to resolve this issue.)

FireEye Label: *Code Execution Through Analysis Of Zip Archives (4 of 5)*
ERNW Paper: 7zip Directory Traversal; File Write To Code Execution (Sections 4.1, 4.2)
Severity: Moderate
Products affected: NX, EX, AX, FX
Credit: Felix Wilhelm of ERNW

A vulnerability allowing limited-privilege code execution on a FireEye appliance by sending a specially crafted Zip archive to the appliance for analysis.

FireEye Label: *Local Privilege Escalation (5 of 5)*
ERNW Paper: Local Privilege Escalation (Section 4.3)
Severity: High
Products affected: NX, EX, AX, FX
Credit: None

A vulnerability in a legacy component, which could allow an attacker with authenticated access to the FireEye Operating System to execute commands to escalate access and gain administrator privileges.

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.