RCE vulnerability in jar analysis

December 15, 2015

On Friday, December 4, 2015, while working with Google Project Zero's Tavis Ormandy and Natalie Silvanovich on the testing of our products as part of our vulnerability disclosure program, FireEye was informed of a Remote Code Execution (RCE) vulnerability that impacted the NX, EX, FX and AX Series products.

On Saturday morning, December 5, 2015, due to the severity of the issue discovered, an automated remediation for this RCE issue was released via our hourly Security Content update process, mitigating any customer exposure. A permanent fix was subsequently released via our Security Content update process on Monday, December 7, 2015.

FireEye Label: Remote code execution vulnerability in jar analysis
Credit: Tavis Ormandy and Natalie Silvanovich
Severity: High
Products Affected: NX, EX, AX, FX
Description:

A vulnerability existed in a module that analyzes Java jar files that could allow an attacker to execute code remotely on a FireEye appliance. Given that remote code execution could be possible, we have concluded in our analysis that this vulnerability posed a high risk to our customers. This issue has been fixed, details below:

Version and Fix Details:

Product	Security content version	Date Released	Customer Actions Required
NX	427.334	12/7/2015	None; Fix applied through automated security content update**
EX	427.334	12/7/2015	None; Fix applied through automated security content update**
AX	427.334	12/7/2015	None; Fix applied through automated security content update**
FX	427.334	12/7/2015	None; Fix applied through automated security content update**

**Customers who perform manual Security Content updates should update immediately.

**We are also making a fix available for out-of-contract customers, for more information please contact our customer support team at support@fireeye.com

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.

We look forward to working with Google and their Project Zero Team to continuously improve our customer protection through research community engagement. We appreciate the support of the security researcher community and encourage responsible disclosure of any potential security issues to 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 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 vulnerabilities in FireEye products, please send an email to security[at]FireEye.com.