SECURITY ADVISORY

April 30th, 2019

Executive Summary:
FireEye would like to recognize the contributions of the security research community. In Q1 of 2019, FireEye remediated several vulnerabilities disclosed by the research community.

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.

FireEye Label: FindFirstFile API Evasion Technique
Credit: Duarte Silva
Severity: High
Products Affected: FireEye AX, FireEye EX, FireEye NX
Description:
An evasion technique was discovered that allowed a malicious file to identify a FireEye appliance using the FindFirstFile API.

Version and Fix Details:

<table>
<thead>
<tr>
<th>Product</th>
<th>Fixed Version</th>
<th>Date Released</th>
<th>Customer Actions Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AX, EX, NX</td>
<td>17R1.9 or later</td>
<td>2019/02/20</td>
<td>Update to latest version</td>
</tr>
</tbody>
</table>

FireEye Label: XSS vulnerability on FireEye website
Credit: Aswin S
Severity: Low
Products Affected: FireEye Partners Website
Description:
Identified a XSS vulnerability on the partners.fireeye.com website.

Version and Fix Details:

<table>
<thead>
<tr>
<th>Product</th>
<th>Fixed Version</th>
<th>Date Released</th>
<th>Customer Actions Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>March 20, 2019</td>
<td>None</td>
</tr>
</tbody>
</table>
We appreciate the support of the security researcher community and encourage responsible disclosure of any potential security issues. We 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

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

To report vulnerabilities in FireEye products, please send an email to security@FireEye.com.

Revision history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>April 30th, 2019</td>
</tr>
</tbody>
</table>

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

For further information, Please visit our Customer Support page at: [http://www.fireeye.com/support/contact-customer-support.html](http://www.fireeye.com/support/contact-customer-support.html)