Security Advisory

August 20st, 2018

Executive Summary:

FireEye has remediated several infrastructure vulnerabilities submitted by external researchers.

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: FireEye EX Bypass
Credit: Steven VanLandingham, Mario Piva, Chris Salerno, Chris Myers
Severity: Medium
Products Affected: FireEye EX
Description:
When processing messages with certain international characters, FireEye EX would not identify the email as malicious.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
FireEye EX	EX 8.1.4	August 2018	Update to latest version

FireEye Label: HSTS preload missing in www.fireeye.com
Credit: Kirtikumar Anandrao Ramchandani
Severity: Low
Products Affected: www.fireeye.com
Description:
Identified a missing HSTS header on www.fireeye.com.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	N/A	None

FireEye Label: RC4 Cipher Suites Detected
Credit: Mohammed Israil
Severity: Low
Products Affected: FireEye University Relations Website
Description:
Insecure TLS ciphers used on a FireEye website.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	N/A	None

FireEye Label: FTP Server Identified
Credit: Meshal Al Mutairi
Severity: Low
Products Affected: FireEye Customer Support
Description:
An FTP server was found being used as an informal site to exchange non-sensitive files. The site was replaced with a more secure file transfer system.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	N/A	None

FireEye Label: Anonymous Write Access on www.fireeye.com
Credit: Ateek Khan
Severity: Low
Products Affected: www.fireeye.com
Description:
The researcher identified a way to anonymous create a file on www.fireeye.com.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	N/A	None

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:

Version	Date
Version 1	August 20, 2018

If you have any questions, please contact FireEye Security at security@fireeye.com

For further information, please visit our Security page at:

https://www.fireeye.com/company/security.html