Security Advisory

March 21, 2017

Executive Summary:

FireEye has issued a set of FireEye Operating Systems (FEOS) updates for the following products: AX. Additionally, FireEye has issued security updates to our operational infrastructure and applications. These updates contain a number of vulnerability fixes credited to researchers other than FireEye.

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: XSS in FireEye Website
Credit: Shwetabh Suman
Severity: Low
Products Affected: FireEye Infrastructure Website
Description:

A cross-side scripting bug existed in the https://ambassadors.fireeye.com web site.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	July 27, 2016	None

FireEye Label: XSS in FireEye ETP Portal
Credit: Jun Kokatsu
Severity: Low
Products Affected: FireEye Infrastructure Website
Description:

A cross-side scripting bug existed in the https://etp.fireeyecloud.com web site.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
ETP	N/A	June 22, 2016	None

FireEye Label: Subdomain takeover
Credit: Ryan Griffin
Severity: Low
Products Affected: FireEye Infrastructure Website
Description:

CNAME entry for a sub-domain was pointing to a third party service.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	February 27, 2017	None

FireEye Label: SQL injection is possible via “Author” section of xlsx file
Credit: Kazufumi Aoki
Severity: Low
Products Affected: AX
Description:

Possible to inject SQL via “Author” section of xlsx file due to lack of sanity check.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
AX	7.7.4 or higher	June 16, 2016	Update to latest version

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	March 21, 2017

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