Security Advisory

October 5th, 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: Added rules to protect the AX when using proxy live mode and live mode
Credit: Andreas Dewald of ERNW
Severity: High
Products Affected: FireEye AX
Description:
A vulnerability existed that allowed a sample to communicate with the network services of the FireEye device with using live mode.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
AX	7.7.7 or higher	August 1st, 2017	Update to latest version

FireEye Label: Obsolete version of PHP in FireEye University Relations Website
Credit: Rafael Fontes Souza
Severity: Medium
Products Affected: FireEye University Relations Website
Description:
Identified an obsolete version of PHP used on the FireEye University Relations Website.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Feb. 13, 2017	None

FireEye Label: Missing Input Validation on www2.fireeye.com
Credit: Babar Khan Akhunzada
Severity: Low
Products Affected: FireEye Marketo Website
Description:
Identified an input validation vulnerability on the www2.fireeye.com website.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	April 14, 2017	None

FireEye Label: AEM-related vulnerabilities on www.fireeye.com
Credit: Cedric Van Bockhaven
Severity: Medium
Products Affected: FireEye Website
Description:
Discovered multiple issues with the FireEye's usage of Adobe Experience Manager (AEM).

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Aug. 2nd, 2017	None

FireEye Label: Untrusted certificate
in docs.fireeye.com & portal-dti.fireeye.com
Credit: Huy Kha
Severity: Low
Products Affected: FireEye Docs and DTI Website
Description:
Found a certificate used by docs.fireeye.com and portal-dti.fireeye.com missing the appropriate intermediary certificates causing it to be listed as untrusted.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
DTI	N/A	Aug 18, 2017	N/A

FireEye Label: Clickjacking Vulnerability on portal-dti.fireeye.com
Credit: Huy Kha
Severity: Low
Products Affected: DTI Website
Description:
Identified an issue with the DTI portal that may lead to a clickjacking attack.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
DTI	N/A	Sep 8, 2017	N/A

FireEye Label: Multiple Stale DNS Entries Identified
Credit: Vineet Kumar
Severity: Low
Products Affected: FireEye DNS
Description:
Multiple unused DNS entries were identified that may have led to a subdomain takeover issue.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
DTI	N/A	Sep 26, 2017	N/A

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	October 5, 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