Security Advisory

January 30th, 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: Redirect Vulnerability in Helix Website
Credit: Amine Tahiri
Severity: Medium
Products Affected: Helix Website
Description:
Identified an invalidated redirect vulnerability in the Helix website.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Jan 2018	None

FireEye Label: Multiple Vulnerabilities in the University Relations Website
Credit: Syed Sohaib Karim
Severity: Low
Products Affected: University Relations Website
Description:
Identified multiple vulnerabilities in the University Relations Website.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Dec 2017	None

FireEye Label: Clickjacking Vulnerabilities on www.fireeye.com
Credit: Mohammed Israil
Severity: Medium
Products Affected: FireEye Website
Description:
Discovered multiple URLs leading to a clickjacking attack.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Oct 2017	None

FireEye Label: Adobe Experience Manager-related vulnerability on www.fireeye.com
Credit: Cedric Van Bockhaven <cedric@ce3c.be>
Severity: Medium
Products Affected: FireEye Website
Description:
AEM-related vulnerability on www.fireeye.com

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Oct. 2017	None

FireEye Label: Security Vulnerability - event-registration.fireeye.com
Credit: Suresh Narvaneni
Severity: Low/Medium
Products Affected: Event Registration Website
Description:
Server Misconfiguration on the Event Registration site.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	Oct. 2017	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 2	January 26, 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