Security Advisory

August 26th, 2019

Executive Summary

FireEye would like to recognize the contributions of the security research community. In Q3 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.

Submissions

FireEye Label: FireEye Endpoint Security on Linux Installation Issue

Credit: Patrick William

Severity: Medium

Products Affected: FireEye Endpoint Security

Description:

Under the right circumstances, a vulnerability was identified that could lead to privilege escalation on Linux.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
HX	Agent 30.19.0	8/27/2019	Update to latest version

FireEye, Inc. I 601 McCarthy Blvd. Milpitas, CA 95035 I 408.321.6300 I 877.FIREEYE (347.3393) I info@fireeye.com I www.fireeye.com

FireEye Label: AEM-related vulnerabilities on www.fireeye.com

Credit: Léandre Forget-Besnard

Severity: Low

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	May 3rd, 2019	None

FireEye Label: Proxy configuration error

Credit: Ninjaninji

Severity: Low

Products Affected: FireEye Website

Description:

A proxy misconfiguration was identified on a FireEye web property.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	April 5th, 2019	None

FireEye Label: HTML injection error on FireEye web site

Credit: Aditya Sharma

Severity: Low

Products Affected: www.fireeye.com

Description:

Identified an HTML injection issue on www.fireeye.com

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
N/A	N/A	April 2nd, 2019	None

FireEye Label: Additional AEM vulnerabilities

Credit: Ahmed Atif

Severity: Low

Products Affected: www.fireeye.com

Description:

Discovered an issue 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	May 3rd, 2019	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	July 26th, 2019
Version 2	August 26th, 2019

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