Security Advisory

February 3rd, 2020

Executive Summary

FireEye would like to recognize the contributions of the security research community. In Q4 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: PowerShell Evasion Technique

Credit: Christoph Falta

Severity: Medium

Products Affected: FireEye Endpoint Security

Description:

The Endpoint Security agent was unable to detect when a console history logging was disabled. This allowed PowerShell commands to execute without being expected by the HX agent.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
HX	SC 358.101	01/09/2020	Update the latest security content

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: Email Security URL Evasion Techniques

Credit: Reegun J

Severity: Low

Products Affected: FireEye Email Security

Description:

A researcher identified two techniques that under certain circumstances could be used to evade detection. The issue was resolved using security content.

FireEye Label: Content Injection on FireEye Website

Credit: Hammad Qureshi

Severity: Low

Products Affected: FireEye Website

Description:

A content injection vulnerability was identified and fixed on the FireEye corporate website.

FireEye Label: Antivirus Unpacker Evasion Technique

Credit: Thierry Zoller

Severity: Low

Products Affected: FireEye Endpoint Security

Description:

A researcher identified a technique that could be used to bypass the antivirus detections in FireEye Endpoint Security. The agent will not unpack corrupted archives even if an end user can unpack them. Since the corrupted archive is not a threat until the malicious content is extracted, FireEye Endpoint agent will alert on the malicious activity once it is extracted from the archive. We believe this protects FireEye Endpoint customers from this threat.

FireEye Label: Endpoint Security Console Session Timeout Issue

Credit: Ashutosh Barot

Severity: Low

Products Affected: FireEye Endpoint Security Console

Description:

The Endpoint Security console will continue displaying important information after a user session is deactivitated due to inactivity.

FireEye Label: Session Invalidation on password Change

Credit: Osama Tariq

Severity: Low

Products Affected: FireEye Network Security

Description:

The user session is not invalidated after a password change.

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	February 3rd, 2020
Version 2	February 5th, 2020

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