ENDPOINT SECURITY

Process Guard

GENERAL AVAILABILITY RELEASE NOTES

RELEASE 1.4.1

Endpoint Security Process Guard Module

Software Release 1.4.1

Revision 1.1

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: https://csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

Announcements

Thank you for using this FireEye Product. This document provides an overview of the new features, resolved issues, and known issues in the FireEye Endpoint Security Process Guard 1.4.1 release.

FireEye Customer Security Best Practices

Because our quality assurance process includes continuous security testing, FireEye recommends updating all FireEye products with the latest releases as soon as possible. As an overall strategy to reduce risk exposure, customers are also encouraged to follow best practices, which include:

- Always keep the product version up to date.
- Limit network access to the management interfaces of the appliance using firewalls or similar measures.
- Only issue accounts to trusted administrators.
- Use strong passwords.
- Monitor logs.
- Restrict physical access to the appliance to trusted administrators.
- Technical preview modules are meant for limited deployments to test environment only, FireEye doesn't recommend for production environment deployments.
- Technical preview modules don't support upgrade to newer versions.
- Technical preview modules don't support upgrading Endpoint Security Server and Agent to newer versions. It is recommended to uninstall technical preview modules before any upgrade.

Process Guard

This release of Process Guard is supported on **Endpoint Security 5.0.0** with **agent 32.30.10 (MR)** running on **Windows 7 and above**. Please read the entire document for dependencies, limitations and known issues for the current release.

Note: This release is supported on Windows platform only. It is not recommended to install Process Guard release 1.4.1 on Endpoint Security Server 4.9.x with agent 32.30.0 or lower versions. This is not a supported scenario.

Features

Process Guard is an HX Innovation Architecture (IA) module designed to prevent attackers from obtaining access to credential data or key material stored within the Windows Local Security Subsystem Service (LSASS) process, thus protecting endpoints against common credential theft attacks. This module provides ability to:

- Enable/Disable LSASS process protection
- Enable/Disable BLOCK on detection capability
- Add Exclusions to whitelist applications
- View Process Guard events
- Integrate with Enricher
- Generate Alerts

Installation Instructions

Process Guard is an optional module available for **Endpoint Security 5.0.0** with **agent 32.30.10 (MR)**. It is installed using the Endpoint Security Web UI by downloading the module installer package (.cms file) from the FireEye Market and then uploading the module .cms file to your Endpoint Security Web UI.

For more details on install and configuration see the Process Guard module user guide, refer to *Part IV: Configuring the Process Guard Module* for steps to enable the server module. After the module is installed successfully, it appears on the Modules menu tab.

Note: If you have non-Windows hosts, FireEye recommends that you exclude them from Process Guard module install because the release 1.4.1 doesn't support mac OS and Linux platforms.

Product Compatibility

This section describes the product compatibility for Process Guard release 1.4.1

Agent Version	Endpoint Security Server Version	Operating System Requirements		
		Windows	macOS	Linux
*32.30.10+	5.0+	Yes	No	No

*Agent 32.0 needs to be updated to MR (32.30.10) release

Supported Windows operating systems:

Windows 7, Windows 8, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

Fixed Issues

The following issues were resolved in the Endpoint Security Process Guard 1.4.1 release and the relevant issue tracking numbers for each item are included in parentheses.

- Unable to export watcher grid, 404 error (ENDPT-50306)
- Unable to save filter set in watcher grid (ENDPT-50368)

Known Issues

- Endpoint Agent Process *"xagt.exe"* instance is detected, and an event reported (ENDPT-67086).

Technical Support

For Technical Preview modules please send email to EndpointTechPreview@fireeye.com

For General Availability modules, contact FireEye through the Support portal https://csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required)
https://docs.fireeye.com