ENDPOINT SECURITY

AMSI

TECHPREVIEW RELEASE NOTES

v1.1.0

AMSI Module

Software Release 1.1.0

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 AMSI module v1.1.0 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.

AMSI

This release of AMSI module is supported on **Endpoint Security 5.0.4** with **Endpoint Agent 32** running on **Windows 10 and above**. AMSI module requires Microsoft Windows AMSI interface on the endpoint to function. Please review Appendix A for dependencies, limitations and known issues for the current release.

Note: This release is supported on Windows 10, Windows Server 2016 and above platforms only.

Features

AMSI module is an HX Innovation Architecture (IA) module designed to provide enhanced malware protection for end user. It detects the execution of malicious scripts using AMSI interface and sends script objects for additional FireEye Endpoint Security scan. This module provides ability to:

- Enable/Disable AMSI feature
- FireEye AMSI rules update interval
- Generate Alerts
- Select confidence threshold for alerting
- Manage database size on the endpoint
- Advanced settings to fine-tune the disk usage and performance

For more details on usage of these feature see the Endpoint Security AMSI module user guide.

Installation Instructions

AMSI module is an optional module available for **Endpoint Security 5.0.4** with **Endpoint Agent v32**. It is installed using your 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. The module is disabled by default.

For more details on install and configuration see the Endpoint Security AMSI module user guide, refer to *Part III: Enabling the AMSI Module* for steps to enable the server module. After you have installed, the module appears on the Modules menu tab

Note: If you have non-Windows hosts, FireEye recommends that you exclude them from AMSI module install because AMSI is available only on Windows OS. Linux and mac OS platforms do not support.

Product Compatibility

This section describes the product compatibility for AMSI Module 1.1.0

Agent Version	Endpoint Security Server Version	Operating System Requirements		
		Windows	macOS	Linux
32.0+	5.0.4+	Yes	No	No

Supported Windows operating systems:

- Windows 10
- Windows Server 2016
- Windows Server 2019

Fixed Issues

The following issues were resolved in the AMSI module release 1.1.0 and the relevant issue tracking numbers for each item are included in parentheses.

- Delay is seen with FireEye AMSI Provider when certain PowerShell commands are executed leading to delays in script execution. (ENDPT-76148)
- AMSI does not generate alerts when malicious scripts are run using Host Remediation module. (ENDPT-77797)

Enhancements

- Support for 32-bit AMSI provider on a 64-bit platform, enabling detection coverage to include both 32 and 64-bit processes.
- Installation and uninstallation enhancements.
- AMSI module installs Microsoft Visual C++ redistributable package (vcredist) as a part of pre-requisite.

Known Issues

The following issues are known in AMSI module release 1.1.0 and the relevant issue tracking numbers for each item are included in parentheses.

- Detection of AMSI bypass techniques is not supported in this release.
- On systems with high AMSI workload, AMSI module is not able to limit the DB size as per the configured value causing excessive disk space usage (ENDPT-87506). Systems referred here could be servers or systems that run PowerShell scripts or any other scripting engine that integrates with AMSI.

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