Configure ESA to Skip Uploading Unknown MIME Type Files to File Analysis Server

Contents

Introduction

This document describes the steps to skip uploading unknown MIME-Type files (Application/octet-stream) to File Analysis Server in Cisco ESA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How Advanced Malware Protection (AMP) in ESA works.
- Basic knowledge of file MIME-types.

Cisco recommends that you have:

- Physical or Virtual ESA Installed.
- License activated or installed.
- The setup wizard is completed.

- Administrative Access to the ESA Command Line Interface (CLI).

Components Used

This document is applicable to AsyncOS 15.5.1, 15.0.2 and later releases.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

MIME Types

A media type, also referred to as a Multipurpose Internet Mail Extensions (MIME) type, serves to identify the character and structure of a document, file, or collection of bytes. The specifications for MIME types are established and made uniform in the Internet Engineering Task Force (IETF) RFC 6838.

Unrecognized subtypes of "text" must be treated as subtype "plain" as long as the MIME implementation knows how to handle the charset. Unrecognized subtypes which also specify an unrecognized charset must be treated as "application/octet- stream".

For more information please refer to RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types

ESA Appliance Exceeded the Upload Limit

If you have enabled the File Analysis service, and the reputation service has no information about the file, and the file meets the criteria for files that can be analyzed, then the message can be quarantined and the file sent for analysis. If you have not configured the appliance to quarantine messages when attachments are sent for analysis, or the file is not sent for analysis, then the message is released to the user.

For more information please refer to the User Guide. User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway - GD (General Deployment) - File Reputation Filtering and File Analysis [Cisco Secure Email Gateway] - Cisco

We have introduced a new CLI command to address the issue of devices with limited file submission quotas prematurely reaching maximum upload capacity due to the ESA submitting excessive files for inspection, . This enhancement has been implemented starting with version 15.5.1 and is also being incorporated into the 15.0.2 Maintenance Release (MR) and subsequent versions.

Caution: For enhanced security, we strongly advise uploading all files as recommended. However, if you deem it essential to bypass this step for specific file types, the provided command enables the option to do so at your discretion. Please proceed with caution, understanding the potential risks involved.

Exclude application/octet-stream MIME Types to Upload to File Analysis

To Exclude the application/octet-stream MIME Types to Upload to File Analysis server for scanning, use these steps:

Step 1. Log in to CLI.

Step 2. run **ampconfig** command

Step 3. Type **unknownmimeoverride** and press enter

Note: **unknownmimeoverride** is a hidden command.

Step 4. Type **N** in answer to "Do you want to send unknown mime for analysis only if their extensions are selected? [N]> "

Step 5. Press Enter to exit the wizard.

Step 6. Commit changes

```
ESA_CLI> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting
```

```
details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> unknownmimeoverride

Do you want to send unknown mime for analysis only if their extensions are selected? [Y]> N

ESA_CLI>  commit
```

Linked Defects and Enhancements

This new feature is introduced due to these Feature Requests and Defects:

- **Behaviour change in HTML and Octet-stream files upload to File Analysis confuses customers.** Cisco bug ID CSCwh61317
- **p7s files are uploaded to File Analysis even if the file type is not selected.** Cisco bug ID CSCwh70476

References

User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway - GD (General Deployment) - File Reputation Filtering and File Analysis [Cisco Secure Email Gateway] - Cisco

RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types