Beheben Sie den Fehler "Nicht scannbare Kategorie = Nachrichtenfehler, Nicht scannbarer Grund = Archivfehler:Die Gesamtgrößenbeschränkung der nicht archivierten Dateien wurde überschritten" in einer ESA.

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für den Fehler "Nicht scanbare Kategorie = Nachrichtenfehler, Nicht scanbarer Grund = Archivfehler: Die Gesamtgröße der nicht archivierten Dateien wurde überschritten" in einer E-Mail-Security-Appliance (ESA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ESA
- Cisco Advanced Malware Protection (AMP)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ESA AsyncOS 11.1.2-023
- ESA AsyncOS 12.0.0-419

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

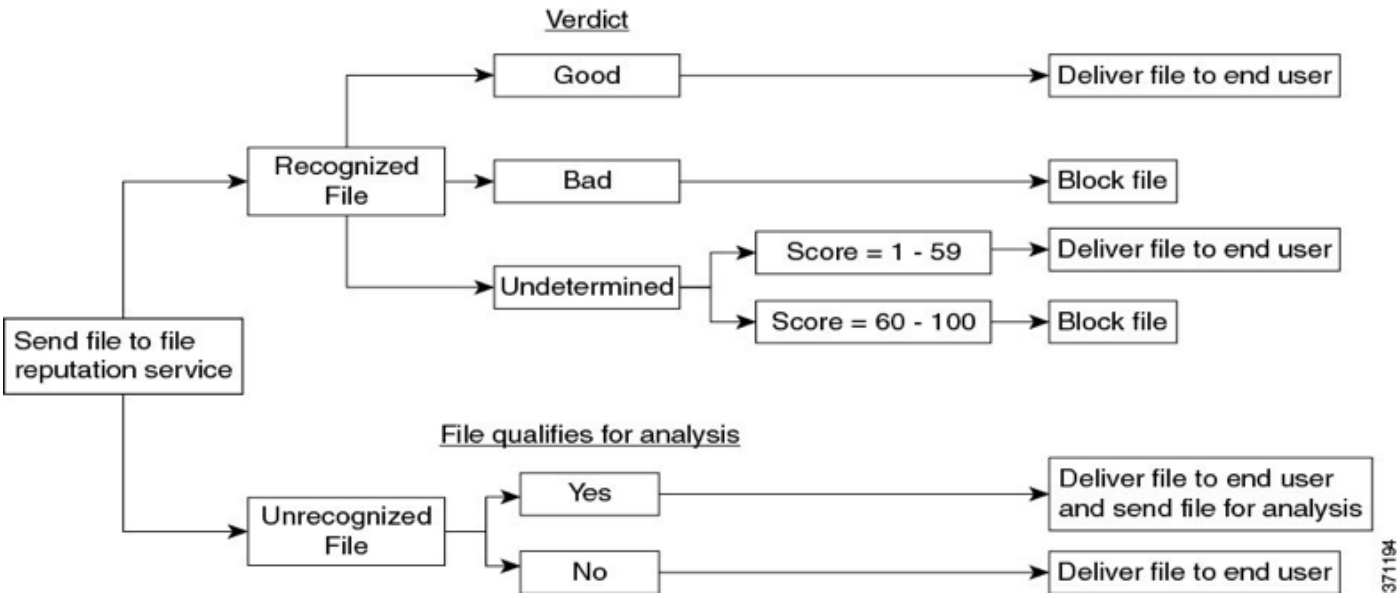
Hintergrundinformationen

Wenn eine Nachricht mit einem Anhang AMP in der Pipeline erreicht, versucht die ESA, den Anhang aus der Nachricht zu analysieren, und überprüft die Nachrichtenheader (Überprüfung auf Konformität mit RFC 2045). Selbst wenn die Nachricht nicht vollständig konform ist, bemüht sich die ESA nach wie vor, den Anhang zu analysieren.

Der nächste Schritt besteht darin, zu überprüfen, ob eine Anlage eine Archivdatei ist. Wenn dies der Fall ist, versucht die ESA, sie zu entpacken, berücksichtigt sie mehrere Faktoren, um die Größe der komprimierten Datei zu bestimmen, um sicherzustellen, dass die Anlage rechtmäßig und keine ZIP-Datei ist.

Wenn keine Dateireputation gefunden wird und die Datei die Kriterien für die Analyse erfüllt, wird sie in Quarantäne verschoben und in die Sandbox hochgeladen.

Dann öffnet die ESA eine Verbindung zu den AMP-Servern und lädt die Datei hoch und wartet auf Verdict-Updates, wie im Bild gezeigt:



ESA liefert ein Urteil auf der Grundlage folgender Szenarien:

- Wenn eine der extrahierten Dateien schädlich ist, gibt der Dateireputations-Service ein Urteil über schädlich für die komprimierte oder die Archivdatei zurück.
- Wenn die komprimierte Datei oder die Archivdatei schädlich ist und alle extrahierten Dateien sauber sind, gibt der Dateireputations-Service ein Urteil über die schädliche Datei für die komprimierte Datei oder die Archivdatei zurück.
- Wenn das Urteil einer der extrahierten Dateien unbekannt ist, werden die extrahierten Dateien optional (sofern konfiguriert und der Dateityp für die Dateianalyse unterstützt wird) zur Dateianalyse gesendet.

- Wenn das Risiko gering ist, dass eine der extrahierten Dateien oder Anhänge erkannt wird, wird die Datei nicht zur Dateianalyse gesendet.
- Wenn die Extraktion einer Datei fehlschlägt, wenn sie dekomprimiert wird, und dann komprimiert wird oder eine Archivdatei erstellt wird, gibt der Dateireputations-Service ein Urteil über die nicht scannbare Datei für die komprimierte oder die Archivdatei zurück. Beachten Sie, dass in diesem Szenario, wenn eine der extrahierten Dateien schädlich ist, der Dateireputations-Service ein Urteil von Malicious für die komprimierte oder die Archivdatei zurückgibt (Malicious Verdict hat Vorrang vor Unscannable Verdict).

Hochkomprimierte Dateien wie csv, xml, txt können die maximale Dateigröße überschreiten, die fest in ESA codiert ist. Komprimierungsalgorithmen wie Lempel-Ziv, erzeugen eine digitale Karte, die die Anzahl und Position der Zeichen im gesamten Dokument zählt, was zu sehr kleinen Dateigrößen führt.

Auf der anderen Seite, Dateien, die Grafiken, Textformat wie pdf, jpg, png enthalten, sind sie nicht auf die gleiche Weise komprimiert, sodass sie fast die ursprüngliche Dateigröße behalten.

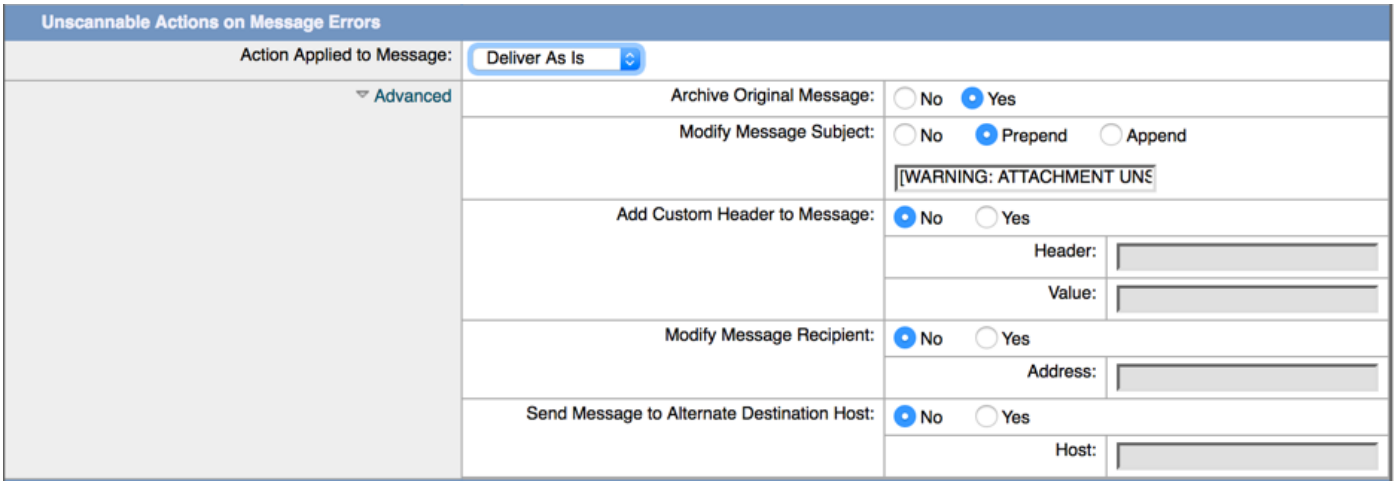
Problem

Wenn die ESA eine E-Mail innerhalb einer Anlage empfängt, die komprimiert ist, und dies das maximale Kompressionsverhältnis überschreitet, und die ESA die Dateigröße der Anlage nicht berechnet, hat dies zur Folge, dass das Fehlerprotokoll:

"Mi Feb 13 20:03:47 2019 Info: Der Anhang konnte nicht gescannt werden. Dateiname = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Nicht scanbare Kategorie = Nachrichtenfehler, Nicht scanbarer Grund = Archivfehler: Die maximale Gesamtgröße der nicht archivierten Dateien wurde überschritten."

Lösung 1

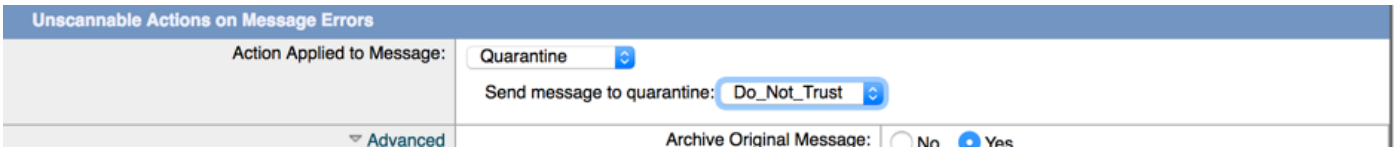
Senden Sie nicht scanbare Nachrichten an den Betreff, um Benutzer zu warnen, dass die Datei nicht von AMP-Services analysiert wurde, wie im Bild gezeigt.



Lösung 2

Nicht scanbare Elemente zur weiteren Analyse in Quarantäne für Policy Virus & Outbreak (PVO)

verschieben. wie im Bild dargestellt.



Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 12.0 für Cisco Email Security Appliances - GD (Allgemeine Bereitstellung)
- Aktivierung von AMP auf Content Security-Produkten (ESA/WSA)
- Dateianalyse-Uploads auf ESA überprüfen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.