

ريغ ةئفل" اهحال صإو أطخلا فاشكتسأ ةلاس ر أطخ = يئوضلا حس ملل ةلباقلا أطخ = يئوضلا حس ملل لباقلا ريغ ببسلا تافل ملل يل امجالا مجحلا دح زواجت: فيشرا ESA في "اهتفشرا متت مل يتلا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [معلومات أساسية](#)
- [المشكلة](#)
- [الحل 1](#)
- [الحل 2](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا وثيقة كيف أن يتحرى الخطأ "UnscanAble Category = رسالة خطأ، unscanAble سبب = أرشفة خطأ: تجاوز الحد الإجمالي لحجم الملفات التي لم تتم أرشفتها" في (Email Security Appliance (ESA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إسا
- الحماية المتقدمة من البرامج الضارة من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

• ESA AsyncOS 11.1.2-023

• ESA AsyncOS 12.0.0-419

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

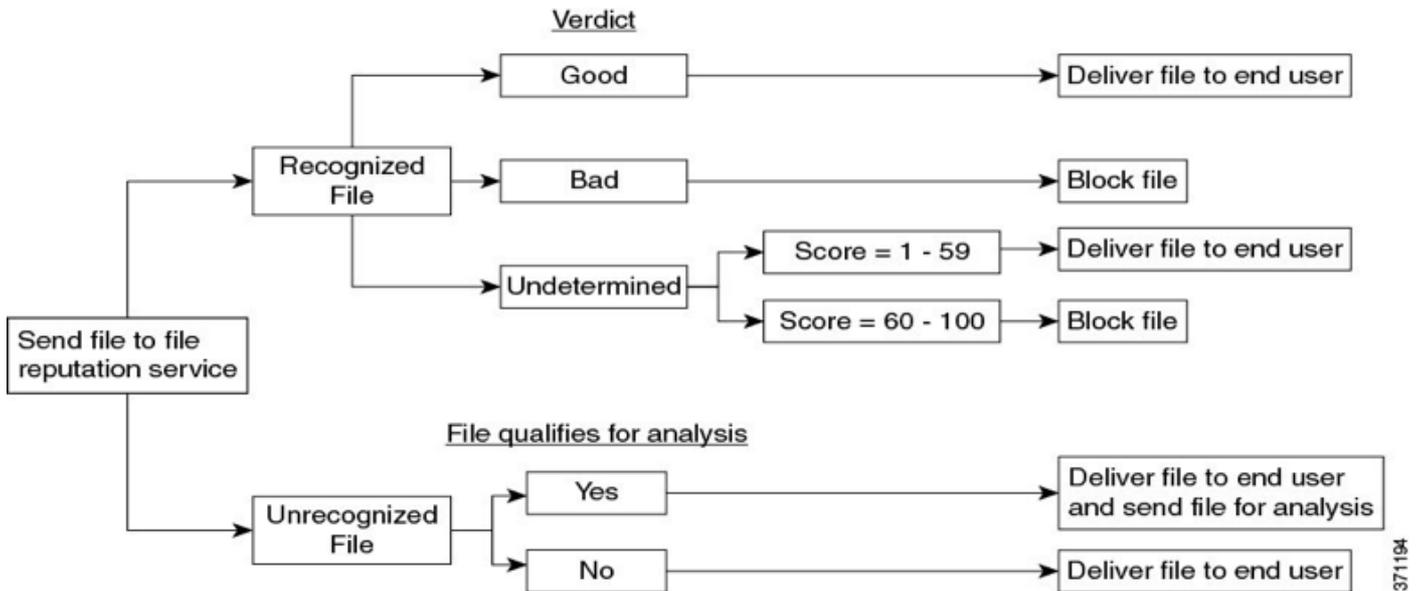
معلومات أساسية

عندما تصل رسالة ذات مرفق إلى AMP في سير العمل، تحاول ESA تحليل المرفق من الرسالة وتحقق من رؤوس الرسائل (تحقق من التوافق مع RFC 2045). وحتى إذا لم تكن الرسالة متوافقة تماما، فإن وكالة الفضاء الأوروبية ما زالت تبذل قصارى جهدها لتحليل المرفق.

تتمثل الخطوة التالية في التحقق مما إذا كان المرفق ملغا أرشيفيا وإذا كان كذلك، تحاول ESA فك حزمه، وتأخذ في الاعتبار عوامل متعددة لتحديد حجم الملف المضغوط للتأكد من أن المرفق قانوني وليس ملف zip.

عند عدم العثور على سمعة الملف، واستيفاء الملف لمعايير التحليل، فإنه يتم وضعه في الحجر الصحي وتحمله إلى المربع المربع المربع.

بعد ذلك، تفتح ESA اتصالا بخوادم AMP وتحميل الملف وتنتظر تحديثات الأحكام، كما هو موضح في الصورة:



وتقدم الإيسا حكما بناء على هذه السيناريوهات:

- إذا كان أحد الملفات المستخرجة ضار، تقوم خدمة سمعة الملف بإرجاع حكم ضار لملف الأرشيف أو مضغوط.
- إذا كان الملف المضغوط أو ملف الأرشيف مضغوطا وكانت جميع الملفات المستخرجة نظيفة، ترجع خدمة سمعة الملف حكما خاطئا على ملف الأرشيف أو المضغوط.
- إذا كان الحكم الصادر عن أي من الملفات المستخرجة غير معروف، فإن الملفات المستخرجة تكون إختيارية (إذا تم تكوينها وكان نوع الملف مدعوما لتحليل الملف) مرسلة لتحليل الملف.
- إذا كان الحكم الخاص بأي من الملفات المستخرجة أو المرفقات منخفض المخاطر، فلا يتم إرسال الملف لتحليل الملف.
- إذا فشل إستخراج الملف عندما يتم فك ضغطه ثم يتم ضغطه أو ملف أرشيف، تقوم خدمة سمعة الملف بإرجاع حكم بعدم المسح الضوئي لملف الأرشيف أو المضغوط. تذكر أنه، في هذا السيناريو، إذا كان أحد الملفات المستخرجة ضار، تقوم خدمة سمعة الملف بإرجاع حكم ضار لملف المضغوط أو ملف الأرشيف (تعطى الأسبقية للحكم الضار على الحكم الذي لا يمكن مسحه).

الملفات المضغوطة بشدة مثل CSV، XML، TXT يمكن أن يتجاوز الحد الأقصى لحجم الملف المرمز ترميزا ثابتا داخل ESA، خوارزميات الضغط، مثل Lempel-ZIV، تولد خريطة رقمية تحسب عدد الحروف وموضعها داخل الوثيقة بأكملها وهذا ينتج أحجام ملفات صغيرة جدا.

من ناحية أخرى، الملفات التي تحتوي على رسومات، تنسيق نص مثل png، jpg، PDF، لا يتم ضغطها بنفس الطريقة، بحيث تحافظ على حجم الملف الأصلي تقريبا.

المشكلة

عندما يستلم ESA بريدًا إلكترونيًا ضمن مرفق مضغوط ويتجاوز هذا النسبة الحد الأقصى لمعدل الضغط ويفشل ESA في حساب حجم ملف المرفق، عندئذ تكون النتيجة هي سجل الأخطاء هذا:

"تم حذف معلومات 13 فبراير 2019 20:03:47: تعذر فحص المرفق. اسم الملف = ACTS Chopped ISO' = 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 = 7efa6154b7519872055cff10a69067dcad8562f708b284a390a9abcf5e99b8f, Ununscan0able = N0able خطأ في الرسالة، السبب غير القابل للمسح = خطأ أرشيف: تجاوز الحد الأقصى للحجم الإجمالي للملفات التي لم تتم أرشفتها

الحل 1

قم بتجهيز الرسائل التي لا يمكن مسحها ضوئيًا في خاضع لمستخدمي التنبيه بأن الملف لم يتم تحليله بواسطة خدمات AMP، كما هو موضح في الصورة.

Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is
Advanced	
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>

الحل 2

الحجر الصحي الذي لا يمكن فحصه في الحجر الصحي الخاص بسياسة مكافحة الفيروسات والتفشي (PVO) لمزيد من التحليل. كما هو موضح في الصورة.

Unscannable Actions on Message Errors	
Action Applied to Message:	Quarantine
Send message to quarantine:	Do_Not_Trust
Advanced	
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes

معلومات ذات صلة

- دليل المستخدم لـ AsyncOS 12.0 لأجهزة أمان البريد الإلكتروني من Cisco - GD (النشر العام)
- تمكين AMP على منتجات أمان المحتوى (ESAWSA)
- التحقق من تحميلات تحليل الملفات على ESA
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلل دن تسمل