تختلف تحديثات مكافحة الفيروسات لجهاز الأمان من Cisco عن تلك المتوفرة على موقع Sophos على الويب

المحتويات

المقدمة

يوضح هذا المستند سبب أختلاف تحديثات Sophos لمكافحة الفيروسات على جهاز أمان Cisco عن تلك المتوفرة على موقع Sophos على الويب.

طلب

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أجهزة أمان البريد الإلكتروني (ESA) (Cisco Email Security Appliance)
- جميع إصدارات AsyncOS

الخلفية

هناك نوعان من التحديثات: تحديثات محرك مكافحة الفيروسات من Sophos وتحديثات ملفات تعريف فيروس Sophos (ملفات بيئة التطوير المتكامل (IDE)).

تم دمج محرك Sophos Anti-virus بالكامل في نظام التشغيل AsyncOS. وتولد شركة Sophos نسخة جديدة من محرك المسح المضاد للفيروسات كل شهر تقريبا. يحتوي الإصدار الجديد على كل من تعريفات الفيروسات الحالية وأي تغييرات في التعليمات البرمجية المطلوبة للتعرف على الأنواع الجديدة من الفيروسات وإصلاح المشكلات المعروفة. مع اكتشاف فيروسات إضافية، Sophos يطلق ملفات تعريف الفيروسات، تسمى ملفات IDE. ستعمل هذه مع محركات عمرها أقل من 90 يوما.

تتم إدارة تحديثات Sophos تلقائيا بواسطة Cisco AsyncOS في جهاز السلسلة C. بما أن Sophos تطلق إصدارات جديدة من المحرك الخاص بها، فإن Cisco تؤهلها من خلال عملية ضمان الجودة (QA)، ثم تضعها على خوادم تحديث Cisco بحيث يقوم جهاز C-Series بتنزيلها وتحديثها تلقائيا. مع إطلاق ملفات تعريف فيروس IDE، ينتقل هذا تلقائيا خلال الخدمة ويتم وضعه على خوادم تحديث Cisco في غضون دقائق قليلة من إصدارها من قبل Sophos.

توقيعات فيروس IDE Sophos صالحة وتعمل باستخدام إصدارات المحرك السابقة. سيتم تحميل جميع IDEs الحالية

وستعمل مع إصدار المحرك الجاري تشغيله في جهاز Cisco C-Series.

التكوين

في بعض الأحيان، قد تبدو الملفات الموجودة على Cisco ESA غير متزامنة مع الملفات المتوفرة مباشرة من Sophos. ويمكن أن يزيد من تعقيد هذا الفارق في المنطقة الزمنية بين Sophos ومعظم عملاء أمريكا الشمالية. ويدير موقع سوفوس على شبكة الإنترنت مقر سوفوس بالقرب من أكسفورد في المملكة المتحدة. وقد تم تحديد المواقع بالزمن مع المنطقة الزمنية المحلية، GMT. من المربك قليلا ربط ملفات Sophos IDE. لا يؤدي أختلاف الوقت الكبير غالبا إلى ظهور التواريخ على أنها يوم منفصل فحسب، بل تستخدم Cisco مخطط ترقيم مختلف لملفات IDE. يمكنك محاولة مطابقة هذه الملفات عن طريق التحقق من موقع Sophos IDE لمعرفة متى تم إصدار IDE، بالإضافة إلى عدد الملفات الأخرى التي تم إصدارها في ذلك اليوم واليوم الذي قبله، ولكن بما أن Cisco ستلتقط غالبا التغييرات المتزايدة التي لم يتم نشرها على هذا الموقع، فإن هذه الطريقة ليست الأكثر فعالية. تستعلم Cisco موقع Sophos على الويب كل 10 دقائق. الإعداد الافتراضي للجهاز هو الاستعلام عن موقع تنزيل Cisco كل خمس دقائق. في أسوأ الحالات سيكون هناك تأخير لمدة 15 دقيقة.

مخطط الترقيم لملفات IDE هو التاريخ. على سبيل المثال، "قواعد Sophos IDE Rules 2004121402 TUE Dec 14:06:27:14 2004" مرتبطة بتحديث ثابت (بدء العد من الصفر) في 14 ديسمبر، نشر هنا.

cisco يوصي أن يثبت أنت ال sophos تلقائيا تحديث فاصل إلى التقصير عملية إعداد من 15 دقيقة. تحقق من أنك تتلقى تحديثات مستمرة من Cisco باستخدام واجهة المستخدم الرسومية (GUI) المستندة إلى الويب، على **خدمات الأمان->**صفحة **مكافحة الفيروسات**. تتوفر هذه المعلومات أيضا باستخدام أمر واجهة سطر الأوامر ((CLI **antivirusstatus**، على سبيل المثال:

```
mail3.example.com> antivirusstatus
SAV Engine Version        4.03
IDE Serial                2006031503
Last Engine Update        Tue Mar 14 01:01:49 2006
Last IDE Update           Thu Mar 16 06:33:50 2006
Last Update Attempt       Thu Mar 16 09:18:51 2006
Last Update Success       Thu Mar 16 06:33:50 2006
```

إذا لم تكن التحديثات ناجحة (ستتلقى رسالة تنبيه إذا حدث ذلك)، فيمكنك تجربة تحديث يدوي باستخدام الزر **تحديث الآن** في واجهة المستخدم الرسومية (GUI)، أو أمر واجهة سطر الأوامر (**antivirusupdate** (CLI. تظهر حالة التحديث في ملف سجل مكافحة الفيروسات. على سبيل المثال:

```
:smtp.example.com> tailCurrently configured logs
antivirus" Module: thirdparty Format: Anti-Virus" .1
avarchive" Module: mail Format: Anti-Virus Archive" .2
bounces" Module: bounces Format: Bounces" .3
brightmail" Module: thirdparty Format: Symantec Brightmail Anti-Spam" .4
cli_logs" Module: system Format: CLI Audit Logs" .5
error_logs" Module: mail Format: IronPort Text" .6
ftpd_logs" Module: ftpd Format: IronPort Text" .7
gui_logs" Module: gui Format: IronPort Text" .8
mail_logs" Module: mail Format: IronPort Text" .9
rptd_logs" Module: rptd Format: IronPort Text" .10
sntpd_logs" Module: sntpd Format: IronPort Text" .11
status" Module: mail Format: Status Logs" .12
system_logs" Module: system Format: IronPort Text" .13
.Enter the number of the log you wish to tail
.1Press Ctrl-C to stop <[]
.Thu Mar 16 09:08:50 2006 Info: Current IDE serial=2006031503. No update needed
Thu Mar 16 09:13:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:13:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
```

```
    .Thu Mar 16 09:13:50 2006 Info: Current IDE serial=2006031503. No update needed
                          Thu Mar 16 09:18:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:18:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
    .Thu Mar 16 09:18:50 2006 Info: Current IDE serial=2006031503. No update needed
                          Thu Mar 16 09:23:50 2006 Info: Checking for Sophos Update
Thu Mar 16 09:23:50 2006 Info: Current SAV engine ver=4.03. No engine update needed
    .Thu Mar 16 09:23:50 2006 Info: Current IDE serial=2006031503. No update needed
                                                                                C^
                                                                <smtp.example.com
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).