Les mises à jour d'antivirus de Sophos sur l'appliance de sécurité Cisco sont différentes de ceux disponibles sur le site Web de Sophos

Contenu

Introduction

Ce document décrit pourquoi les mises à jour d'antivirus de Sophos sur l'appliance de sécurité Cisco sont différentes que ceux disponibles sur le site Web de Sophos.

Prerequiste

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Toutes les versions d'AsyncOS

Fond

Il y a deux types de mises à jour : mises à jour à l'engine d'antivirus de Sophos et mises à jour aux fichiers d'identité de virus de Sophos fichiers (d'Integrated Development Environment (ide)).

L'engine d'antivirus de Sophos est entièrement intégrée dans le système d'exploitation d'AsyncOS. Sophos génère une nouvelle version de leur engine de lecture d'antivirus approximativement tous les mois. La nouvelle version contient les définitions en cours de virus et toutes les modifications du code qui sont exigées pour identifier de nouveaux types de virus et pour réparer des problèmes connus. Pendant que des virus supplémentaires sont découverts, Sophos publie des fichiers d'identité de virus, appelés l'ide classe. Ceux-ci fonctionneront avec les engines qui sont moins de 90 jours de.

Des mises à jour de Sophos sont gérées automatiquement par Cisco AsyncOS dans l'appliance de série C. Car Sophos libère de nouvelles versions de leur engine, Cisco les qualifie par un procédé de l'assurance qualité (QA), et puis les place sur les serveurs de mise à jour de Cisco de sorte que votre appliance de série C automatiquement les télécharge et mette à jour. Pendant que

des fichiers de définition de virus ide sont relâchés, ceux-ci se déplacent automatiquement par le service et sont placés sur les serveurs de mise à jour de Cisco à quelques minutes de leur release par Sophos.

Les signatures de virus de Sophos ide sont valides et fonctionnent avec les versions précédentes d'engine. Toutes les ides en cours seront chargées et fonctionneront avec l'exécution de version d'engine dans l'appliance de série C de Cisco.

Configurez

Parfois les fichiers sur Cisco ESA peuvent sembler être hors de synchronisation avec ces fournis directement par Sophos. Ceci peut être encore compliqué par la différence de fuseau horaire entre Sophos et la plupart des clients nord-américains. Le site Web de Sophos est géré par des sièges sociaux de Sophos près d'Oxford au R-U. Les publications sur le site sont datées avec le fuseau horaire local, GMT. Il un peu confond pour corréler des fichiers de Sophos ide. Non seulement la grande différence de temps fait-elle souvent sembler les dates un jour à part, mais Cisco utilise un schéma différent de numérotation pour les fichiers ide. Vous pouvez essayer de sélectionner ces fichiers en vérifiant le site de Sophos ide pour voir quand un ide a été relâché, aussi bien que combien d'autres ont été relâchés que le jour et la veille de lui, mais comme Cisco prendra souvent les modifications incrémentales non signalées sur ce site, ce n'est pas la plupart de méthode efficace. Cisco questionne le site Web de Sophos toutes les 10 minutes. La valeur par défaut pour une appliance est de questionner Cisco téléchargent le site toutes les cinq minutes. Dans le pire des cas il y aura un retard de 15 minutes.

Le schéma de numérotation pour les fichiers ide est la date. Par exemple, « Sophos ide ordonne 2004121402 Tue corrélations du 14 décembre 06:27:14 2004" à la troisième mise à jour (début comptant de zéro) sur Decemeber 14ème, édité ici.

Cisco recommande que vous placiez l'intervalle automatique de mise à jour de Sophos à la valeur par défaut de 15 minutes. Vérifiez que vous obtenez les mises à jour continues de Cisco à l'aide du GUI basé sur le WEB, à la page de **Services->Anti-Virus de Sécurité**. Ces informations sont également disponibles utilisant la commande CLI d'**antivirusstatus**, par exemple :

```
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
```

Si vos mises à jour ne sont pas réussies (vous recevrez un message d'alerte si ceci se produit), vous pouvez essayer une mise à jour manuelle utilisant la **mise à jour** vous boutonnez **maintenant** dans le GUI, ou la commande CLI d'**antivirusupdate**. Le statut de la mise à jour est affiché dans le fichier journal d'antivirus. Exemple :

```
smtp.example.com> tailCurrently configured logs:
1. "antivirus" Module: thirdparty Format: Anti-Virus
2. "avarchive" Module: mail Format: Anti-Virus Archive
3. "bounces" Module: bounces Format: Bounces
4. "brightmail" Module: thirdparty Format: Symantec Brightmail Anti-Spam
5. "cli_logs" Module: system Format: CLI Audit Logs
```

```
6. "error_logs" Module: mail Format: IronPort Text
7. "ftpd_logs" Module: ftpd Format: IronPort Text
8. "gui_logs" Module: gui Format: IronPort Text
9. "mail_logs" Module: mail Format: IronPort Text
10. "rptd_logs" Module: rptd Format: IronPort Text
11. "sntpd_logs" Module: sntpd Format: IronPort Text
12. "status" Module: mail Format: Status Logs
13. "system_logs" Module: system Format: IronPort Text
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>
```