Las actualizaciones del contra virus de Sophos en el dispositivo del Cisco Security son diferentes de ésas disponibles en el sitio web de Sophos

Contenido

Introducción

Este documento describe porqué las actualizaciones del contra virus de Sophos en el dispositivo de seguridad de Cisco son diferentes que ésas disponibles en el sitio web de Sophos.

Prerequiste

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad del correo electrónico de Cisco (ESA)
- Todas las versiones de AsyncOS

Antecedente

Hay dos tipos de actualizaciones: actualizaciones al motor antivirus de Sophos y actualizaciones a los archivos de la identidad del virus de Sophos (archivos del entorno de desarrollo integrado (IDE)).

El motor antivirus de Sophos es completamente integrado en el sistema operativo de AsyncOS. Sophos genera una nueva versión de su motor de análisis del contra virus aproximadamente cada mes. La nueva versión contiene ambas definiciones de virus actuales y cualquier cambio del código que se requieran reconocer los tipos nuevos de virus y reparar los problemas conocidos. Mientras que se descubren los virus adicionales, Sophos libera los archivos de la identidad del virus, llamados IDE clasifía. Éstos trabajarán con los motores que son menos de 90 días de viejo.

Las actualizaciones de Sophos son manejadas automáticamente por Cisco AsyncOS en el dispositivo de la serie C. Pues Sophos libera las nuevas versiones de su motor, Cisco las califica

con un proceso de la garantía de calidad (QA), y después las pone en los servidores de actualización de Cisco de modo que su dispositivo de la serie C los descargue y ponga al día automáticamente. Mientras que se liberan los archivos de definición de virus IDE, éstos se mueven automáticamente con el servicio y son colocados en los servidores de actualización de Cisco a unos minutos de su versión por Sophos.

Las firmas de virus de Sophos IDE son válidas y actúan con las versiones anteriores del motor. Todos los IDE actuales serán cargados y trabajarán con la versión del motor que se ejecuta en el dispositivo de la serie C de Cisco.

Configurar

Los archivos en Cisco ESA pueden aparecer a veces estar fuera de sincronización con esos disponibles directamente de Sophos. Esto se puede complicar más a fondo por la diferencia del timezone entre Sophos y la mayoría de los clientes norteamericanos. El sitio web de Sophos es manejado por las jefaturas de Sophos cerca de Oxford en el UK. Las fijaciones en el sitio se fechan con la Zona horaria local, GMT. Un poco está confundiendo para correlacionar los archivos de Sophos IDE. No sólo la diferencia de tiempo grande hace a menudo las fechas parecer un día aparte, pero Cisco utiliza un diverso esquema de la enumeración para los archivos IDE. Usted puede intentar hacer juego estos archivos marcando el sitio de Sophos IDE para ver cuando un IDE fue liberado, así como cuántos otros fueron liberados que el día y el día antes de él, sino como Cisco a menudo cogerá los cambios ampliados no fijados en este sitio, éste no es la mayoría del método eficiente. Cisco pregunta el sitio web de Sophos cada 10 minutos. La configuración predeterminada para un dispositivo es preguntar el sitio de descarga de Cisco cada cinco minutos. En el peor de los casos habrá un retardo de 15 minutos.

El esquema de la enumeración para los archivos IDE es la fecha. Por ejemplo, “Sophos IDE las reglas 2004121402 Tue el 14 de diciembre 06:27:14 el 2004" correlaciona a la tercera actualización (comienzo que cuenta a partir de la cero) en Decemeber 14to, publicado aquí.

Cisco recomienda que usted fija el intervalo automático de la actualización de Sophos a la configuración predeterminada de 15 minutos. Compruebe que usted está consiguiendo las actualizaciones continuas de Cisco usando el GUI basado en web, la página de **Services->Anti-Virus de la Seguridad**. Esta información está también disponible con el comando CLI del **antivirusstatus**, por ejemplo:

```
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 sus actualizaciones no son acertadas (usted recibirá un mensaje de alerta si sucede éste), usted puede intentar una actualización manual usando la **actualización ahora** abotona en el GUI, o el comando CLI del **antivirusupdate**. El estatus de la actualización se muestra en el archivo del registro del antivirus. Por ejemplo:

```
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>
```