As atualizações anti-vírus de Sophos no dispositivo do Cisco Security são diferentes daquelas disponíveis no site de Sophos

Índice

Introdução

Este documento descreve porque as atualizações anti-vírus de Sophos na ferramenta de segurança de Cisco são diferentes do que aquelas disponíveis no site de Sophos.

Prerequiste

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco envia por correio eletrónico a ferramenta de segurança (o ESA)
- Todas as versões de AsyncOS

Background

Há dois tipos de atualizações: atualizações ao motor anti-vírus de Sophos e atualizações aos arquivos da identidade do vírus de Sophos (arquivos integrados do ambiente de desenvolvimento (IDE)).

O motor anti-vírus de Sophos é integrado inteiramente no sistema operacional de AsyncOS. Sophos gerencie uma nova versão de seu motor anti-vírus da exploração aproximadamente cada mês. A nova versão contém ambas as definições de vírus atuais e todas as mudanças do código que forem exigidas para reconhecer novos tipos de vírus e para fixar problemas conhecidos. Enquanto os vírus adicionais são descobertos, Sophos libera os arquivos da identidade do vírus, chamados IDE arquiva. Estes trabalharão com motores que são menos de 90 dias velho.

As atualizações de Sophos são controladas automaticamente por Cisco AsyncOS no dispositivo da série C. Porque Sophos libera novas versões de seu motor, Cisco qualifica-as com um processo da garantia de qualidade (QA), e coloca-as então nos server da atualização de Cisco de modo que seu dispositivo da série C automaticamente os transfira e atualize. Enquanto os

arquivos de definição de vírus IDE são liberados, estes movem-se automaticamente com o serviço e estão colocados nos server da atualização de Cisco a poucos minutos de sua liberação por Sophos.

As assinaturas de vírus de Sophos IDE são válidas e operam-se com as versões precedentes do motor. Todo o IDEs atual será carregado e trabalhará com a versão do motor que é executado no dispositivo da série C de Cisco.

Configurar

Às vezes os arquivos em Cisco ESA podem parecer ser fora da sincronização com aqueles disponíveis diretamente de Sophos. Isto pode mais ser complicado pela diferença do fuso horário entre Sophos e a maioria de clientes norte-americanos. O site de Sophos é controlado por matrizes de Sophos perto de Oxford no UK. As postagens no local são datadas com o fuso horário local, GMT. Um pouco está confundindo para correlacionar arquivos de Sophos IDE. Não somente a grande diferença de horário faz com frequentemente que as datas pareçam um dia distante, mas Cisco usa um esquema diferente da numeração para os arquivos IDE. Você pode tentar combinar estes arquivos verificando o local de Sophos IDE para ver quando um IDE foi liberado, assim como quanto outro foi liberado que o dia e o dia antes dele, mas como Cisco pegararão frequentemente as mudanças incrementais não afixadas neste local, este não é a maioria de método eficiente. Cisco pergunta o Web site de Sophos os minutos cada 10. A configuração padrão para um dispositivo é perguntar Cisco transfere o local cada cinco minutos. Na pior das hipóteses haverá um atraso de 15 minutos.

O esquema da numeração para os arquivos IDE é a data. Por exemplo, “Sophos IDE as regras 2004121402 Terça-feira o 14 de dezembro 06:27:14 2004" correlaciona à terceira atualização (começo que conta de zero) em Decemeber 14o, publicado aqui.

Cisco recomenda que você ajusta o intervalo automático da atualização de Sophos à configuração padrão de 15 minutos. Certifique-se de você esteja obtendo atualizações contínuas de Cisco usando o GUI com base na Web, na página de **Services->Anti-Virus da Segurança**. Esta informação está igualmente disponível usando o comando CLI do **antivirusstatus**, por exemplo:

```
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
```

Se suas atualizações não são bem sucedidas (você receberá um mensagem de alerta se este acontece), você pode tentar uma atualização manual que usa a **atualização** abotoa-se **agora no** GUI, ou no comando CLI do **antivirusupdate**. O estado da atualização é mostrado no arquivo de registro do antivirus. Por exemplo:

```
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>
```