Gli aggiornamenti antivirus Sophos su Cisco Security Appliance sono diversi da quelli disponibili sul sito Web Sophos

Sommario

Introduzione

Questo documento descrive i motivi per cui gli aggiornamenti antivirus Sophos sull'appliance di sicurezza Cisco sono diversi da quelli disponibili sul sito Web Sophos.

Prerequisito

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Email Security Appliance (ESA)
- Tutte le versioni di AsyncOS

Sfondo

Esistono due tipi di aggiornamenti: aggiornamenti al motore antivirus Sophos e aggiornamenti ai file di identità dei virus Sophos (file IDE).

Il motore antivirus Sophos è completamente integrato nel sistema operativo AsyncOS. Sophos genera una nuova versione del motore di scansione antivirus circa ogni mese. La nuova versione contiene sia le definizioni dei virus correnti sia le modifiche al codice necessarie per riconoscere i nuovi tipi di virus e per risolvere i problemi noti. Quando vengono individuati altri virus, Sophos rilascia file di identità dei virus, denominati file IDE. Questi funzionano con motori che hanno meno di 90 giorni.

Gli aggiornamenti Sophos vengono gestiti automaticamente da Cisco AsyncOS nell'accessorio serie C. Quando Sophos rilascia nuove versioni del motore, Cisco le qualifica tramite un processo di controllo qualità (QA) e le inserisce sui server di aggiornamento Cisco in modo che l'appliance serie C le scarichi e le aggiorni automaticamente. Quando vengono rilasciati i file di definizione dei virus IDE, questi si spostano automaticamente attraverso il servizio e vengono posizionati sui

server di aggiornamento Cisco entro pochi minuti dalla loro pubblicazione da parte di Sophos.

Le firme dei virus Sophos IDE sono valide e funzionano con le versioni del motore precedenti. Tutti gli IDE correnti verranno caricati e funzioneranno con la versione del motore in esecuzione nell'accessorio Cisco serie C.

Configurazione

A volte i file sull'ESA Cisco possono sembrare non sincronizzati con quelli disponibili direttamente da Sophos. La differenza di fuso orario tra Sophos e la maggior parte dei clienti nordamericani può ulteriormente complicare questa situazione. Il sito web di Sophos è gestito dalla sede centrale di Sophos vicino ad Oxford, in Gran Bretagna. I messaggi sul sito sono datati con il fuso orario locale, GMT. Correlare i file IDE di Sophos è un po' confuso. Non solo la grande differenza di orario spesso fa apparire le date un giorno distanti, ma Cisco utilizza uno schema di numerazione diverso per i file IDE. È possibile cercare di trovare una corrispondenza tra questi file controllando il sito IDE Sophos per vedere quando un IDE è stato rilasciato, così come quanti altri sono stati rilasciati quel giorno e il giorno prima, ma poiché Cisco prenderà spesso le modifiche incrementali non pubblicate su questo sito, questo non è il metodo più efficiente. Cisco invia una query al sito Web Sophos ogni 10 minuti. Per impostazione predefinita, un accessorio esegue una query sul sito di download di Cisco ogni cinque minuti. Nel peggiore dei casi ci sarà un ritardo di 15 minuti.

Lo schema di numerazione per i file IDE è la data. Ad esempio, "Sophos IDE Rules 2004121402 Tue Dec 14 06:27:14 2004" è correlato al terzo aggiornamento (a partire da zero) del 14 dicembre, pubblicato qui.

Cisco consiglia di impostare l'intervallo di aggiornamento automatico di Sophos sull'impostazione predefinita di 15 minuti. Verificare di ricevere aggiornamenti continui da Cisco tramite l'interfaccia utente grafica basata sul Web nella pagina **Security Services->Anti-Virus**. Queste informazioni sono disponibili anche usando il comando **antivirusstatus** CLI, ad esempio:

```
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 gli aggiornamenti non riescono (se ciò accade, viene visualizzato un messaggio di avviso), è possibile provare a eseguire un aggiornamento manuale utilizzando il pulsante **Aggiorna ora** nella GUI o il comando **antivirus** Update CLI. Lo stato dell'aggiornamento è indicato nel file registro antivirus. Ad esempio:

```
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>
```