Dit soort anti-virusupdates over Cisco security applicatie is anders dan de updates die beschikbaar zijn op de website Sofo's

Inhoud

Inleiding

In dit document wordt beschreven waarom de updates van Sofo's Anti-Virus op het Cisco security apparaat verschillen van die op de Sofo's website.

Prerequiste

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco e-mail security applicatie (ESR)
- Alle versies van AsyncOS

Achtergrond

Er zijn twee soorten updates: updates van de Sofs Anti-Virus motor en updates van de Sofs virus Identity files (Integrated Development Environment (IDE) bestanden).

De anti-virusmotor van Sofs is volledig geïntegreerd in het AsyncOS-besturingssysteem. Sofobs genereert ongeveer iedere maand een nieuwe versie van hun antivirusscanning-machine. De nieuwe versie bevat zowel de huidige virusdefinities als alle codeputaties die nodig zijn om nieuwe typen virussen te herkennen en bekende problemen op te lossen. Aangezien er nog meer virussen worden ontdekt, geeft Sofs de identiteitsbestanden van het virus vrij, IDE-bestanden genaamd. Deze zullen werken met motoren die jonger zijn dan 90 dagen.

Snoepupdates worden automatisch door Cisco AsyncOS in het c-Series apparaat beheerd. Aangezien Sofs nieuwe versies van hun motor afgeeft, kwalificeert Cisco deze door een QA-proces (Quality assurance) en plaatst ze deze op de update servers van Cisco, zodat uw C-Series apparaat ze automatisch downloaden en bijwerken. Aangezien de definitiebestanden van het IDE-virus worden vrijgegeven, verplaatsen deze zich automatisch door de service en worden deze

binnen een paar minuten na hun release door Sofo's op de Cisco-update-servers geplaatst.

Sofs IDE-virushandtekeningen zijn geldig en werken met de vorige motorversies. Alle huidige IDE's worden geladen en werken met de motorversie die in het Cisco C-Series-apparaat werkt.

Configureren

Soms lijken de bestanden op Cisco ESA niet te zijn gesynchroniseerd met de bestanden die direct beschikbaar zijn via Sofo's. Dit kan nog worden gecompliceerd door het tijdsverschil tussen Sofo's en de meeste Noord-Amerikaanse klanten. De website Sofs wordt beheerd door het Sofos hoofdkantoor in de buurt van Oxford in het Verenigd Koninkrijk. De berichten op de site zijn gedateerd met de lokale tijdzone GMT. Het is een beetje verwarrend om Sofo's IDE-bestanden met elkaar te correleren. Niet alleen veroorzaakt het grote tijdverschil vaak de datums om een dag uit elkaar te lijken, maar Cisco gebruikt een ander nummeringsschema voor de IDE-bestanden. U kunt proberen deze bestanden te matchen door de SofoS IDE-site te controleren om te zien wanneer een IDE is uitgebracht en hoeveel anderen die dag en de dag ervoor zijn vrijgelaten, maar omdat Cisco vaak incrementele veranderingen zal oppikken die niet op deze site zijn geplaatst, is dit niet de meest efficiënte methode. Cisco stelt elke 10 minuten vragen over de website van Sofs. De standaardinstelling voor een apparaat is om de vijf minuten een vraag te stellen naar de Cisco-downloadsite. In het ergste geval is er een vertraging van 15 minuten.

Het nummeringsschema voor de IDE-bestanden is de datum. Bijvoorbeeld, "Sofs IDE Rules 2004121402 Tue dec 14 06:27:14 2004" correleert met de derde update (begin te tellen vanaf nul) op 14 december, hier gepubliceerd.

Cisco raadt u aan om het Soos Automatic Update Interval in te stellen op de standaardinstelling van 15 minuten. Controleer of u ononderbroken updates van Cisco krijgt door het gebruik van de op web-gebaseerde GUI, op de pagina **Security Services-Anti-Virus**. Deze informatie is ook beschikbaar onder de opdracht **antivirale status** CLI, bijvoorbeeld:

```
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
```

Als uw updates niet geslaagd zijn (u ontvangt een waarschuwingsbericht als dit gebeurt), kunt u een handmatige update proberen met behulp van de knop **Update Now** in de GUI, of de opdracht **antivirus update** CLI. De status van de update wordt weergegeven in het anti-viruslogbestand. Bijvoorbeeld:

```
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>
```