思科安全裝置上的Sophos防病毒更新與Sophos網站上提供的更新不同

目錄

簡介

本文檔說明思科安全裝置上的Sophos防病毒更新與Sophos網站上的更新不同的原因。

前提條件

思科建議您瞭解以下主題：

- 思科電子郵件安全裝置(ESA)
- AsyncOS的所有版本

背景

更新有兩種型別：更新Sophos防病毒引擎並更新Sophos病毒標識檔案(整合開發環境(IDE)檔案)。

Sophos防病毒引擎完全整合到AsyncOS作業系統中。Sophos大約每個月都會生成其防病毒掃描引擎的新版本。新版本既包含當前的病毒定義，也包含識別新型別的病毒和解決已知問題所需的任何代碼更改。在發現其他病毒時，Sophos會發佈稱為IDE檔案的病毒標識檔案。這些適用於使用不到90天的引擎。

Sophos更新由C系列裝置中的Cisco AsyncOS自動管理。當Sophos發佈其引擎的新版本時，思科會通過品質保證(QA)流程對這些引擎進行鑑定，然後將其放到思科更新伺服器上，以便您的C系列裝置自動下載並更新這些引擎。發佈IDE病毒定義檔案後，這些檔案將自動通過該服務移動，並在Sophos發佈後幾分鐘內放置在思科更新伺服器上。

Sophos IDE病毒簽名有效，並可使用以前的引擎版本運行。所有當前的IDE都將載入，並適用於在思科C系列裝置中運行的引擎版本。

設定

有時，Cisco ESA上的檔案可能與Sophos直接提供的檔案不同步。由於Sophos和大多數北美客戶的時區差異，這種情況可能會更加複雜。Sophos網站由英國牛津附近的Sophos總部管理。該站點上的帖子標註了當地時區GMT的日期。將Sophos IDE檔案關聯起來有點混亂。較大的時間差不僅通常導致日期看起來相隔一天，而且Cisco對IDE檔案使用不同的編號方案。您可以通過檢查Sophos IDE站點來嘗試匹配這些檔案，以檢視IDE發佈的時間，以及當天和前一天的已發佈其他檔案數量。但是，由於思科經常會獲取未發佈在此站點上的增量更改，因此這不是最有效的方法。思科每10分鐘查詢一次Sophos網站。裝置的預設設定為每五分鐘查詢一次思科下載站點。最壞的情況是15分鐘的延遲。

IDE檔案的編號方案是日期。例如，「Sophos IDE Rules 2004121402 Tue Dec 14 06:27:14 2004」與12月14日發佈的第三次更新（從零開始計數）相關，發佈於此處。

思科建議您將Sophos自動更新間隔設定為預設設定15分鐘。在**Security Services**->Anti-Virus頁面，使用基於Web的GUI檢查您是否從Cisco獲得持續更新。也可使用**antivirusstatus** CLI命令獲取此資訊，例如：

```
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
```

如果更新失敗（如果發生這種情況，您將收到警告消息），則可以嘗試使用GUI中的**Update Now**按鈕或**antivirusupdate** CLI命令進行手動更新。更新的狀態顯示在防病毒日誌檔案中。例如：

```
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>
```