從思科安全端點刪除過時的Windows排除

目錄

簡介

本文檔介紹從Windows安全終端客戶環境中刪除常見錯誤排除的計畫流程。

問題描述

為了儘可能降低對效能的影響並最大限度地提高思科安全終端的功能性，我們的工程師已經確定了客戶環境中存在的最常見的過時排除，並將在2022年10月將其刪除。安全端點（6.x及更早版本）的先前版本依賴萬用字元功能(*)來利用多驅動器排除。後來對排除定義和輸入進行了更改和改進，消除了這種寬泛格式的需要，並且調整了思科維護的排除以解決萬用字元建立的效能影響。隨著Windows Secure Endpoint 7.5.3的發佈，允許萬用字元(*)進程排除的一項新功能，改變了星號前導排除的處理，導致在其環境中仍具有以下排除的客戶的cpu消耗增加：

```
*\Windows\Security\database\*.sdb
*\Windows\Security\database\*.edb
*\Windows\Security\database\*.chk
*\Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\Security\database\*.jrs
*\Windows\Security\database\*.log
*\Windows\Temp\content.zip.tmp\*.diff
*\Windows\Temp\content.zip.tmp\cur.scr
*\Windows\Temp\TMP*.tmp
*\Windows\Temp\musdmys_*
*\Windows\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
*.sas*
*\Windows\SoftwareDistribution\Datastore\Logs\edb*.log
*\System Volume Information\tracking.log
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*\*.tmp
*\Program Files (x86)\SysTrack\LsiAgent\Condense\*\*.hld
*\Windows\Temp\AltirisScript*.cmd
*\Windows\System32\drivers\*-*.tmp
*\Users\*\AppData\Local\Temp\*-*.tmp
*\Users\*\AppData\Local\Temp\warsaw_*
*\Windows\Temp\warsaw_*
*Windows\SoftwareDistribution\Datastore\Logs\*.log
*\Windows\System32\Dns\*.dns
*\Windows\System32\DNS\*.scc
*\Windows\ntds\EDB*.log
*\Windows\ntds\Edbres*.jrs
*\Windows\ntds\*.pat
*\Windows\SoftwareDistribution\Datastore\Logs\edb.log
*\Windows\Security\database\.edb
```

```
*\Windows\Security\database\.jrs
*\Windows\Security\database\.log
*\Windows\Security\database\.sdb
*Windows\Temp\mus*
*Windows\Temp\content.zip.tmp*
```

其他步驟

刪除這些排除項不會對您的環境產生負面影響，並可以提高使用Windows安全終端7.5.3及更高版本的主機的效能。如果需要多個驅動器，請檢視當前自定義排除清單，瞭解任何星號前導(*)排除項，並修改這些排除項，以使用萬用字元可用的「應用於所有驅動器號」功能，否則，請在路徑中提供驅動器號。如果您使用下列任何軟體，請確保將思科維護清單新增到策略中，因為已準備好正確的排除項以供使用：

- Microsoft Windows預設值
- 賽門鐵克的Altiris
- 域控制器
- 迪博爾德華沙
- Lakeside軟體 — 系統
- SAS應用
- 賽門鐵克

附註：如果您的組織內存在與凍結更改相關的顧慮，請最遲在2022年10**月1日開啟TAC案例並參考本文。**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。