Entfernen veralteter Windows-Ausschlüsse aus Cisco Secure Endpoint

Inhalt

[Einleitung](#)
[Problembeschreibung](#)
[Weitere Schritte](#)

Einleitung

In diesem Dokument wird der geplante Prozess zum Entfernen gängiger, missgestalteter Ausschlüsse aus der Windows Secure Endpoint-Kundenumgebung beschrieben.

Problembeschreibung

In dem Bestreben, die Auswirkungen auf die Leistung zu minimieren und die Funktionalität von Cisco Secure Endpoint zu maximieren, haben unsere Techniker die häufigsten veralteten Ausschlüsse in unserer Kundenumgebung ermittelt und werden sie im Laufe des Monats Oktober 2022 entfernen. Frühere Versionen von Secure Endpoint (6.x und früher) nutzten die Platzhalterfunktion (*), um Ausschlüsse für mehrere Laufwerke zu nutzen. Durch spätere Änderungen und Verbesserungen der Ausschlussdefinition und -eingabe entfiel die Notwendigkeit eines solchen breiten Formats, und die von Cisco verwalteten Ausschlüsse wurden angepasst, um die Leistungseinbußen zu beheben, die durch die Platzhalter verursacht wurden. Mit der Einführung von Windows Secure Endpoint 7.5.3 wurde eine neue Funktion für Ausschlüsse von Platzhalterprozessen (*) eingeführt, die die Handhabung von Ausschlüssen mit Sternchen veränderte und zu einem Anstieg des CPU-Verbrauchs bei Kunden führte, die in ihrer Umgebung noch immer die folgenden Ausschlüsse hatten:

```
*\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\Temp\mus*
*Windows\Temp\content.zip.tmp*
```

Weitere Schritte

Das Entfernen dieser Ausschlüsse hat keine nachteiligen Auswirkungen auf Ihre Umgebung und kann die Leistung auf Hosts mit Windows Secure Endpoint 7.5.3 und höher erhöhen. Bitte überprüfen Sie Ihre aktuellen benutzerdefinierten Ausschlusslisten für alle Asterisk-führenden (*) Ausschlüsse und ändern Sie sie, um die Funktion "Auf alle Laufwerksbuchstaben anwenden" zu verwenden, die für Platzhalter verfügbar ist, wenn Sie mehrere Laufwerke benötigen, oder geben Sie einen Laufwerksbuchstaben im Pfad an, wenn dies nicht der Fall ist. Wenn Sie eine der folgenden Software verwenden, stellen Sie sicher, dass Sie der Richtlinie die Liste der von Cisco verwalteten Geräte hinzufügen, da die richtigen Ausschlüsse bereits vorhanden sind:

- Microsoft Windows-Standard
- Altiris von Symantec
- Domänencontroller
- Diebold Warsaw
- Lakeside Software - Systrack
- SAS-Anwendungen
- Symantec

Hinweis: Wenn Sie Bedenken hinsichtlich des Einfrierens von Änderungen in Ihrem Unternehmen haben, öffnen Sie ein TAC-Ticket, und verweisen Sie **spätestens am 7. Oktober 2022 auf** diesen Artikel.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.