Rimozione di esclusioni di Windows obsolete da Cisco Secure Endpoint

Sommario

Introduzione

In questo documento viene descritto il processo pianificato per la rimozione delle esclusioni dal formato non valido dall'ambiente del cliente di Windows Secure Endpoint.

Descrizione del problema

Nel tentativo costante di ridurre al minimo l'impatto sulle prestazioni e ottimizzare le funzionalità di Cisco Secure Endpoint, i nostri tecnici hanno identificato le esclusioni più diffuse e obsolete presenti nel nostro ambiente cliente e le rimuoveranno nel mese di ottobre 2022. Le iterazioni precedenti di Secure Endpoint (6.x e versioni precedenti) si basano sulla funzionalità dei caratteri jolly (*) per utilizzare le esclusioni di più unità. Modifiche successive e miglioramenti alla definizione e all'input dell'esclusione hanno eliminato la necessità di un formato così ampio e le esclusioni gestite da Cisco sono state adattate per risolvere l'impatto sulle prestazioni creato dai caratteri jolly. Con la release di Windows Secure Endpoint 7.5.3, una nuova funzionalità ha consentito l'esclusione dei processi con caratteri jolly (*), che ha modificato la gestione delle esclusioni che precedono l'asterisco e ha causato un aumento del consumo di CPU per i clienti che ancora avevano le seguenti esclusioni nel loro ambiente:

```
*\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*
```

Ulteriori passaggi

La rimozione di queste esclusioni non influisce negativamente sull'ambiente e può aumentare le prestazioni sugli host che utilizzano Windows Secure Endpoint 7.5.3 e versioni successive. Esaminare gli elenchi di esclusione personalizzati correnti per individuare eventuali esclusioni con asterisco iniziale (*) e modificarli in modo che utilizzino la funzionalità "applica a tutte le lettere di unità" disponibile per i caratteri jolly se sono necessarie più unità o, in caso contrario, fornire una lettera di unità nel percorso. Se si utilizza uno dei seguenti software, assicurarsi di aggiungere l'elenco di prodotti mantenuti da Cisco alla policy, in quanto sono già presenti le esclusioni corrette da utilizzare:

- Impostazioni predefinite di Microsoft Windows
- Altiris di Symantec
- Controller di dominio
- Diebold Varsavia
- Software Lakeside - Systrack
- Applicazioni SAS
- Symantec

Nota: in caso di dubbi relativi al congelamento delle modifiche all'interno dell'organizzazione, aprire una richiesta TAC e fare riferimento a questo articolo **entro il 7 ottobre 2022.**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).