Suppression des exclusions Windows obsolètes de Cisco Secure Endpoint

Table des matières

Introduction

Ce document décrit le processus planifié de suppression des exclusions malformées courantes de l'environnement client Windows Secure Endpoint.

Description du problème

Dans un effort continu pour minimiser l'impact sur les performances et optimiser les fonctionnalités de Cisco Secure Endpoint, nos ingénieurs ont identifié les exclusions obsolètes les plus courantes présentes dans notre environnement client et les supprimeront au cours du mois d'octobre 2022. Les itérations précédentes de Secure Endpoint (6.x et antérieures) utilisaient la fonctionnalité générique (*) pour utiliser les exclusions multilecteurs. Des modifications et améliorations ultérieures apportées à la définition et à l'entrée des exclusions ont éliminé le besoin d'un format aussi large et les exclusions maintenues par Cisco ont été ajustées pour tenir compte de l'impact sur les performances créé par les caractères génériques. Avec la sortie de Windows Secure Endpoint 7.5.3, une nouvelle fonctionnalité a permis d'exclure des processus génériques (*), ce qui a modifié le traitement des exclusions avec astérisque et a entraîné une augmentation de la consommation de CPU pour les clients qui avaient toujours les exclusions suivantes dans leur environnement :

```
*\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*
```

Étapes supplémentaires

La suppression de ces exclusions n'a pas d'impact négatif sur votre environnement et peut augmenter les performances sur les hôtes utilisant Windows Secure Endpoint 7.5.3 et versions ultérieures. Veuillez vérifier vos listes d'exclusions personnalisées actuelles pour toute exclusion avec astérisque (*) et les modifier pour utiliser la fonctionnalité « Appliquer à toutes les lettres de lecteur » disponible pour les caractères génériques si vous avez besoin de plusieurs lecteurs, ou fournir une lettre de lecteur dans le chemin d'accès si ce n'est pas le cas. Si vous utilisez l'un des logiciels suivants, veillez à ajouter la liste de maintenance Cisco à la politique, car les exclusions correctes sont déjà en place pour une utilisation :

- Microsoft Windows par défaut
- Altiris de Symantec
- Contrôleur de domaine
- Diebold Varsovie
- Logiciel Lakeside - Systrack
- Applications SAS
- Symantec

Remarque : si vous avez des doutes concernant le gel des modifications au sein de votre organisation, veuillez ouvrir un dossier TAC et consulter cet article **au plus tard le 7 octobre 2022.**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.