Remoção de exclusões desatualizadas do Windows do Cisco Secure Endpoint

Contents

Introduction

Este documento descreve o processo planejado para remover exclusões malformadas comuns do ambiente do cliente do Windows Secure Endpoint.

Descrição do problema

Em um esforço contínuo para minimizar o impacto no desempenho e maximizar a funcionalidade do Cisco Secure Endpoint, nossos engenheiros identificaram as exclusões desatualizadas mais prevalentes presentes no ambiente do cliente e as removerão durante o mês de outubro de 2022. Iterações anteriores do Secure Endpoint (6.x e anteriores) contavam com a funcionalidade de caractere curinga (*) para a utilização de exclusões de várias unidades. Alterações e melhorias posteriores na definição de exclusão e entrada removeram a necessidade de um formato tão amplo e as Exclusões Mantidas da Cisco foram ajustadas para lidar com o impacto de desempenho que os curingas criaram. Com o lançamento do Windows Secure Endpoint 7.5.3, um novo recurso permitiu exclusões de processos com caracteres curinga (*), o que mudou o tratamento das exclusões com asterisco e causou um aumento no consumo de cpu para clientes que ainda tinham as seguintes exclusões em seu 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*
```

Etapas adicionais

A remoção dessas exclusões não afeta negativamente seu ambiente e pode aumentar o desempenho em hosts que usam o Windows Secure Endpoint 7.5.3 e superior. Verifique suas listas de exclusão personalizadas atuais para ver se há exclusões líderes de Asterisco (*) e modifique-as para usar a funcionalidade "aplicar a todas as letras de unidade" disponível para curingas se precisar de várias unidades ou forneça uma letra de unidade no caminho, caso contrário. Se você usar qualquer um dos softwares a seguir, certifique-se de adicionar a Lista de Mantidos da Cisco à política, pois as exclusões corretas já estão em vigor para uso:

- Padrão do Microsoft Windows
- Altiris da Symantec
- Controlador de domínio
- Diebold Warsaw
- Software Lakeside - Systrack
- Aplicativos SAS
- Symantec

Observação: se houver preocupações relacionadas ao congelamento de alterações em sua organização, abra um caso de TAC e consulte este artigo **até 7 de outubro de 2022.**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.