Verwijdering van verouderde Windows-uitsluitingen uit Cisco Secure Endpoint

Inhoud

[Inleiding](#)
[Probleembeschrijving](#)
[Aanvullende stappen](#)

Inleiding

In dit document wordt het geplande proces beschreven voor het verwijderen van veelvoorkomende mislukte uitsluitingen uit de Windows Secure Endpoint-klantomgeving.

Probleembeschrijving

In een voortdurende inspanning om de impact van prestaties te minimaliseren en de functionaliteit van Cisco Secure Endpoint te maximaliseren, hebben onze engineers de meest voorkomende verouderde uitsluitingen in onze klantenomgeving geïdentificeerd en zullen ze in de maand oktober 2022 verwijderen. Eerdere herhalingen van het Secure Endpoint (6.x en eerder) berustten op de functionaliteit van een jokerteken (*) om meerdere stations uit te sluiten. Latere wijzigingen en verbeteringen in de definitie van uitsluiting en input verwijderden de noodzaak van een dergelijk breed formaat en de Cisco Maintained Exclusions werden aangepast om het effect van de jokertekens op de prestaties te adresseren. Met de release van Windows Secure Endpoint 7.5.3, is een nieuwe functie toegestaan voor uitsluiting van jokerteken (*)-processen, waardoor de verwerking van toonaangevende asterisk-uitsluitingen is gewijzigd en het cpu-verbruik is toegenomen voor klanten die nog steeds de volgende uitsluitingen in hun omgeving hadden:

```
*\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*
```

Aanvullende stappen

Het verwijderen van deze uitsluitingen heeft geen negatieve invloed op uw omgeving en kan de prestaties op hosts verbeteren met behulp van Windows Secure Endpoint 7.5.3 en hoger. Controleer uw huidige aangepaste uitsluitingslijsten voor alle sterretjes-leidende (*) uitsluitingen en wijzig ze om de "Apply to all drive letters"-functionaliteit te gebruiken die beschikbaar is voor wildcards als u meerdere stations nodig hebt, of geef een drive letter in het pad als dat niet het geval is. Als u een van de volgende software gebruikt, zorg er dan voor dat u de handhaven Cisco-lijst aan het beleid toevoegt, aangezien de juiste uitsluitingen al van kracht zijn voor gebruik:

- Standaard Microsoft Windows
- Altiris van Symantec
- Domeincontroller
- Diebold Warschau
- Lakeside Software - Systrack
- SAS-toepassingen
- Symantec

  Opmerking: als er binnen uw organisatie bezorgdheid is over wijzigingsbevriezing, open dan een TAC-case en verwijs **uiterlijk op 7 oktober 2022 naar** dit artikel.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.