Removal of Outdated Windows Exclusions from Cisco Secure Endpoint

Contents

Introduction
Problem Description
Additional Steps

Introduction

This document describes the planned process for removing common malformed exclusions from the Windows Secure Endpoint customer environment.

Problem Description

In an ongoing effort to minimize performance impact and maximize functionality of Cisco Secure Endpoint, our engineers have identified the most prevalent outdated exclusions present in our customer environment and will be removing them during the month of October, 2022. Previous iterations of the Secure Endpoint (6.x and earlier) relied on the wildcard functionality (*) to utilize multi-drive exclusions. Later changes and improvements to exclusion definition and input removed the need for such a broad format and the Cisco Maintained Exclusions were adjusted to address the performance impact that the wildcards created. With the release of Windows Secure Endpoint 7.5.3, a new feature allowed for wildcard (*) process exclusions, which changed the handling of asterisk-leading exclusions and caused an increase in cpu consumption for customers that still had the following exclusions in their environment:

```
*\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*
```

Additional Steps

The removal of these exclusions does not negatively impact your environment and can increase performance on hosts using Windows Secure Endpoint 7.5.3 and above. Please review your current custom exclusion lists for any Asterisk-leading (*) exclusions and modify them to use the "apply to all drive letters" functionality available for wildcards if you need multiple drives, or provide a drive letter in the path if not. If you use any of the following software, please make sure to add the Cisco Maintained List to the policy, as the correct exclusions are already in place for use:

- Microsoft Windows Default
- Altiris by Symantec
- Domain Controller
- Diebold Warsaw
- Lakeside Software - Systrack
- SAS Applications
- Symantec

> **Note**: If there are concerns relating to Change Freeze within your organization, please open a TAC case and reference this article **no later than October 7, 2022.**