面向终端的AMP控制台的思科维护的排除列表更改

目录

2020年7月15日 — 2020年
域控制器 — Windows
Microsoft团队 — Windows
新建列表已创建
2020年8月26日 — 2020年
Microsoft SQL Server - Windows
2020年9月30日 — 2020年
恶意软件字节 — Windows
数字卫报 — Mac
新建列表已创建
2021年3月3日 — 2021年
卡巴斯基 — Windows
SCCM - Windows
Symantec - Windows
新建列表已创建

简介

本文档介绍添加到思科维护的例外项的更改。

思科维护的例外项由思科创建和维护，以便在面向终端的高级恶意软件防护(AMP)连接器和防病毒、安全或其他软件之间提供更好的兼容性，这些例外项可以添加到应用的新版本。

作者：思科工程师Caly Hess。

先决条件

要求

Cisco 建议您了解以下主题：

- 面向终端的AMP中的排除项
- AMP控制台

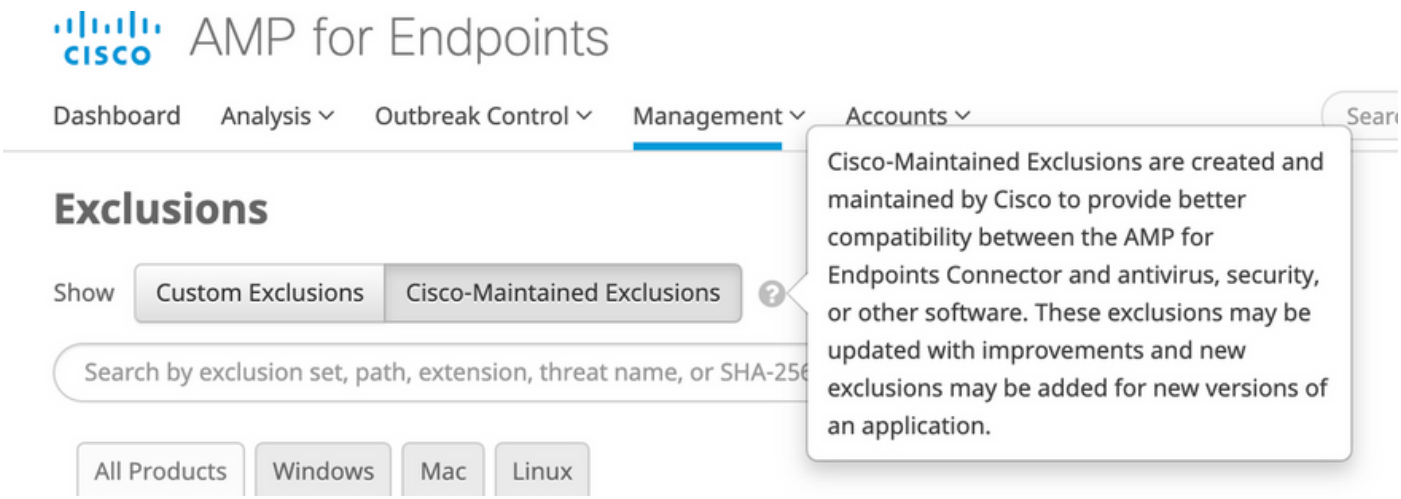
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 面向终端的AMP控制台版本5.4.20190820

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

更新时的期望



当思科维护的列表发生更改时，会在后端执行策略更新以反映该更改。 当每个终端在其心跳上使用该列表签入时，它们会提取更新的策略。 这些策略更改不会反映在审核日志中，因为从技术上讲，它是对排除列表的更改，而不是策略本身，并且思科维护的排除列表在单个控制台的正常审核日志中不存在。 对于大规模环境，这看起来像是大量策略更新，最终结果是每个终端的性能都更好。

更新周期取决于每个终端。 如果所有计算机都在线，更新将在1-2个心跳内进行。 如果这是全局环境，则更新会随着计算机联机而继续发生，因此在推送维护列表24-48小时后不要惊讶地看到其他策略更新。

更改

2019年8月28日 — 2019年

Microsoft Windows默认值：

删除：

- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\edb*.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log**
- **CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log**

理由：重复。基础集中的另一个排除项将其覆盖。

添加：

- **C:\$WINDOWS.~BT\Sources\SetupHost.exe**

理由：由于进程扫描，Windows 10更新偶尔会失败。

N-able Solar Winds - Windows:

添加：

- **C:\Program Files (x86)\N-able Technologies\Windows Agent\bin\agent.exe**
- **C:\Program Files (x86)\BeAnywhere支持Express\GetSupportService_N-Central\BASupSrvc.exe**
- **C:\Program Files (x86)\N-able Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe**

Docker - Mac:

删除：

- **/Users/*/Library/Containers/com.docker.docker/Data/vms/*/Docker.***
- **/usr/local/bin/docker**

原因: 其他测试让我们对安全性感到担忧，因此开发中已找到更好的排除项。

添加：

- /Applications/Docker.app/Contents/MacOS/Docker
- /Applications/Docker.app/Contents/Resources/bin/docker

新列表已创建：

Linux:

- Docker — 连接器1.10.2
- Docker — 连接器1.11+
- 扎比

Mac:

- 虚拟机
- 数字卫报

2019年9月18日 — 2019年

Apple MacOS默认值：

添加：

- /Applications/Time Machine.app/Contents/MacOS/Time Machine
- /System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight

McAfee - Mac

添加：

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

- /usr/bing/grep
- /bin/ps

- //Cisco Jabber.app//MacOS/Cisco Jabber

Crashplan - Mac

添加：

- /Applications/CrashPlan.app/Contents/Library/LaunchServices/CrashPlanService.app/Contents/MacOS/CrashPlanService

JAMF Casper - Mac

删除：

- /usr/bin/sw_vers

添加：

- /库/应用程序Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/目录/MacOS/JamfDaemon
- /usr/local/jamf/bin/jamfAgent
- /usr/local/jamf/bin/jamf
- /库/应用程序Support/JAMF/Jamf.app/Contents/MacOS/JamfAgent.app/目录/MacOS/JamfAgent

VMWare Fusion - Mac

添加：

- /Applications/VMware Fusion.app/Contents/MacOS/VMware Fusion

Xcode - Mac

添加：

- /Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBBuildService.bundle/Contents/MacOS/XCBBuildService
- /Applications/Xcode.app/Contents/Developer/usr/bin/xcodebuild

一个驱动器 — Windows

轻微更改：

- C:*\Users\OneDrive\（添加反斜线以提高安全性）

Citrix ICA客户端 — Windows

添加：

- CSIDL_PROGRAM_FILES\Citrix\User Profile Manager\UserProfileManager.exe
- CSIDL_PROGRAM_FILES\Citrix\Virtual Desktop Agent\BrokerAgent.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\picaSvc2.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\CpSvc.exe

理由： Citrix建议排除的最新更新。

新列表已创建：

Windows 窗口版本

- Citrix调配服务器
- Citrix云连接器

2019年12月11日

一个驱动器 — Windows

添加：

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

添加：

- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe
- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe

Splunk - Linux

添加：

- /opt/splunkforwarder/bin/splunk
- /opt/splunk/bin/splunk

新列表已创建：

Azure - Linux

流浪者 — 麦克

2020年2月12日至20日

Microsoft Windows默认 — Windows

添加：

- C:\Program Files\Cisco\Orbital\osqueryd.exe
- C:\Program Files\Cisco\Orbital\orbital-ampwin.exe

Websense - Windows

添加：

- [多个驱动器]:\Program Files*\Websense\
- C:\Program Files (x86)\Websense\Websense Endpoint\dserui.exe
- C:\Program Files\Websense\Websense Endpoint\dserui.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\EndPointClassifier.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\FilterSDK\kvoop.exe
- C:\Program Files (x86)\Websense\Websense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

添加：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL\FTDATA\
- .sql

2020年6月10日 — 2020年

恶意软件字节 — Windows

轻微更改：

- C:\ProgramData\Malwarebytes Endpoint Agent\
- C:\ProgramData\Malwarebytes\MBAMService\

Microsoft Office - Windows

添加：

- C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe

IIS - Windows

添加：

- C:\Windows\SysWOW64\inetsrv\w3wp.exe
- C:\Windows\System32\inetsrv\w3wp.exe

Symantec Altiris - Windows

添加：

- C:\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe

McAfee - Windows

添加：

- C:\Program Files\McAfee\Endpoint Security\Adaptive Threat Protection\mfeatp.exe

新列表已创建：

NetScout - Windows

IBM - Windows

2020年7月15日 — 2020年

域控制器 — Windows

添加：

- CSIDL_WINDOWS\System32\dfsr.exe
- CSIDL_WINDOWS\System32\dfsrs.exe
- CSIDL_WINDOWS\System32\dns.exe
- CSIDL_WINDOWS\System32\ntfrs.exe

Microsoft团队 — Windows

添加：

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\teams.exe
- CSIDL_LOCAL_APPDATA\Microsoft\Teams\update.exe

新建列表已创建

控制

2020年8月26日 — 2020年

**由于其他测试，原始发布日期从19日延长到26日

Microsoft SQL Server - Windows

更换：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer\Bin\ReportingServicesService.exe

添加：

- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.11\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe

2020年9月30日 — 2020年

恶意软件字节 — Windows

添加：

- CSIDL_PROGRAM_FILES\Malwarebytes' Anti-Malware\mbam.exe
- CSIDL_PROGRAM_FILESX86\Malwarebytes' Anti-Malware\mbam.exe

数字卫报 — Mac

添加：

- /usr/local/dgagent
- /dgagent

新建列表已创建

数字卫报 — Windows

2021年3月3日 — 2021年

卡巴斯基 — Windows

添加：

- CSIDL_PROGRAM_FILESX86\Kaspersky Lab\Kaspersky Endpoint Security for Windows\avp.exe
- CSIDL_PROGRAM_FILESX86\Kaspersky Lab\NetworkAgent\klnagent.exe

SCCM - Windows

删除：

- **WINDOWS\CCM\ServiceData — 重复路径**
- **程序文件\Microsoft Configuration Manager\EasySetupPayload — 重复路径**

Symantec - Windows

添加：

- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\edpa.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.4013.4013.105\Bin64\Smc.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.6600.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7385.6902.105\Bin\ccSvcHst.exe**
- **CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection**
- **CSIDL_PROGRAM_FILES\Symantec\Endpoint Agent\brkrprcs64.exe**

新建列表已创建

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows