# 排除安全终端中的漏洞防御故障

## 目录



## 简介

本文档介绍在安全终端控制台中配置漏洞防御引擎以及如何执行基本分析。

## 先决条件

### 要求

思科建议您了解这些主题。

- 对安全终端控制台的管理员访问权限
- 安全终端连接器
- 已启用漏洞防御功能

### 使用的组件

本文档中的信息基于以下软件和硬件版本。

- 连接器版本7.3.15或更高版本
- Windows 10版本1709及更高版本或Windows Server 2016版本1709及更高版本

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。

## 背景信息

本文档中介绍的过程有助于您根据控制台中触发的事件，执行基本分析，并在您知道该过程并在您

的环境中使用该过程时，建议您使用防漏洞例外项。

利用漏洞防御引擎能够保护您的终端免受恶意软件通常使用的内存注入攻击，以及其他针对未修补软件漏洞的零日攻击。当检测到对受保护进程的攻击时，它会阻止并生成事件，但不会将其隔离。

## 受保护的进程

漏洞防御引擎保护这些32位和64位（安全终端Windows连接器6.2.1版及更高版本）进程及其子进程：

- Microsoft Excel应用程序
- Microsoft Word应用程序
- Microsoft PowerPoint应用程序
- Microsoft Outlook应用程序
- Internet Explorer浏览器
- Mozilla Firefox浏览器
- Google Chrome浏览器
- Microsoft Skype应用程序
- TeamViewer应用程序
- VLC媒体播放器应用
- Microsoft Windows脚本主机
- Microsoft Powershell应用程序
- Adobe Acrobat Reader应用程序
- Microsoft注册服务器
- Microsoft任务计划程序引擎
- Microsoft运行DLL命令
- Microsoft HTML应用程序主机
- Windows脚本主机
- Microsoft程序集注册工具
- 缩放
- 松弛
- Cisco Webex团队
- Microsoft Teams

## 排除的进程

由于兼容性问题，这些进程从漏洞防御引擎中排除（未监控）：

- McAfee DLP服务
- McAfee Endpoint Security实用程序

## 漏洞防御版本5（连接器版本7.5.1及更高版本）

安全终端Windows连接器7.5.1包含漏洞防御的重要更新。此版本的新功能包括：

- 保护网络驱动器：自动保护从网络驱动器运行的进程免受勒索软件等威胁
- 保护远程进程：自动保护使用域身份验证用户(admin)的受保护计算机上远程运行的进程
- 通过rundll32的AppControl旁路：停止允许运行解释命令的经特殊设计的rundll32命令行

- UAC旁路：阻止恶意进程提升权限，从而防止Windows用户帐户控制机制绕过
- 浏览器/Mimikatz电子仓库凭证：如果启用，Exploit Prevention可防止Microsoft Internet Explorer和Edge浏览器中的凭证被盗
- 卷影副本删除：跟踪卷影副本的删除，并拦截Microsoft卷影复制服务(vssvc.exe)中的COM API
- SAM散列：防止Mimikatz窃取SAM散列凭证，拦截枚举和解密注册表配置单元Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users中的所有SAM散列的尝试

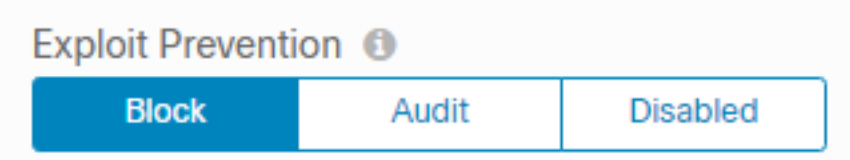
- 保护已执行的进程：如果运行进程在防漏洞攻击实例之前已启动(explorer.exe、lsass.exe、spoolsv.exe、winlogon.exe)，则插入这些进程

在策略中启用Exploit Prevention时，默认情况下这些功能全部启用。

# 配置

要启用Exploit Prevention引擎，请导航到策略中的**Modes and Engines**，然后选择Audit mode、Block mode或Disabled模式，如图所示。

> **注意：**审核模式仅在安全终端Windows连接器7.3.1及更高版本上可用。早期版本的连接器将审核模式视为与块模式相同。

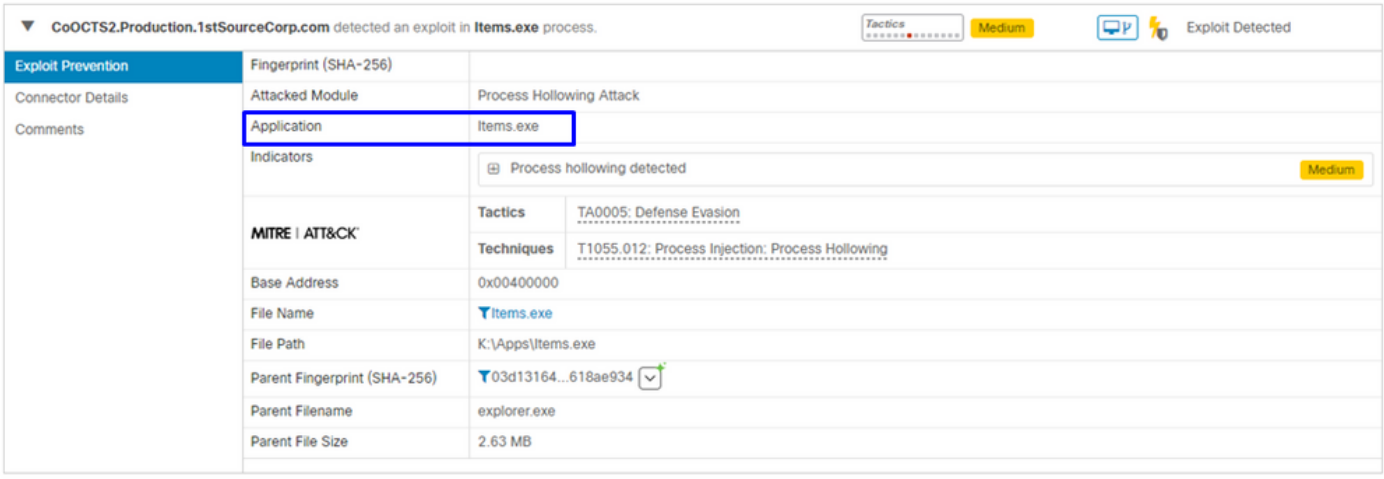



> **注意：**在Windows 7和Windows Server 2008 R2上，在安装连接器之前，需要应用Microsoft安全建议303929的修补程序。

# 检测

触发检测后，终端会显示弹出通知，如图所示。

控制台会显示一个防漏洞事件，如图所示。

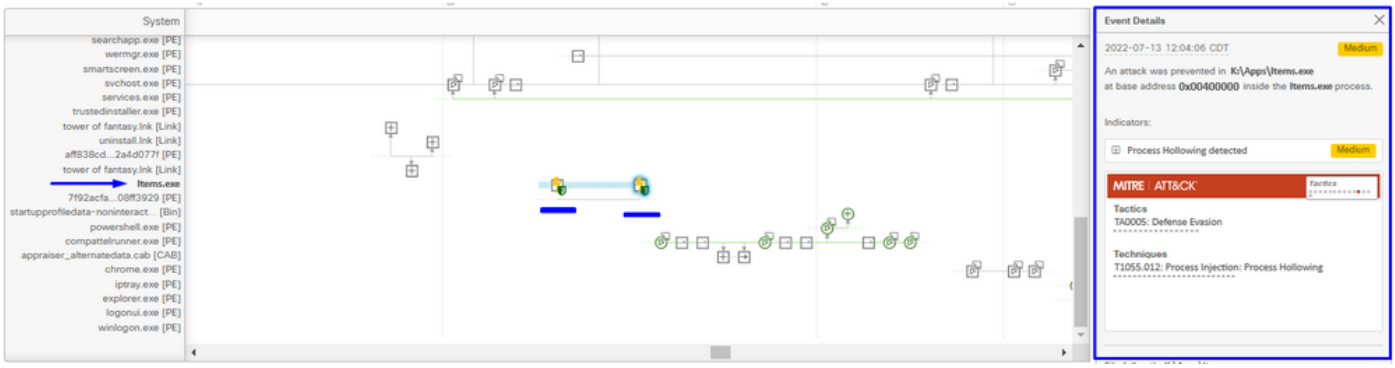


# 故障排除

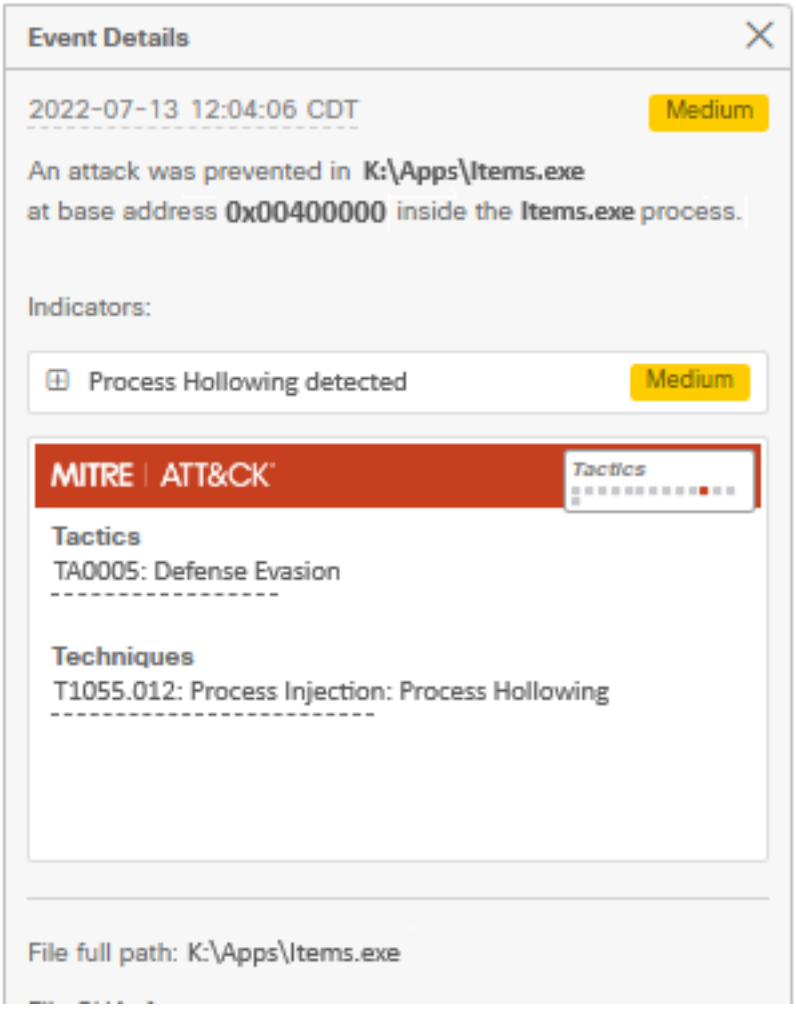
当控制台中触发漏洞防御事件时，识别检测到的进程的方法是基于详细信息以提供对应用程序或进程运行时所发生事件的可视性，您可以导航到**Device Trajectory**。

步骤1.点击Exploit Prevention事件中显示的**Device Trajectory**图标，如图所示。


步骤2.在Device Trajectory的时间表中找到Exploit Prevention图标，以查看**Event Details**部分，如图所示。




步骤3.确定事件的详细信息，并评估您的环境中是否信任/了解该流程或应用程序。




## 误报检测

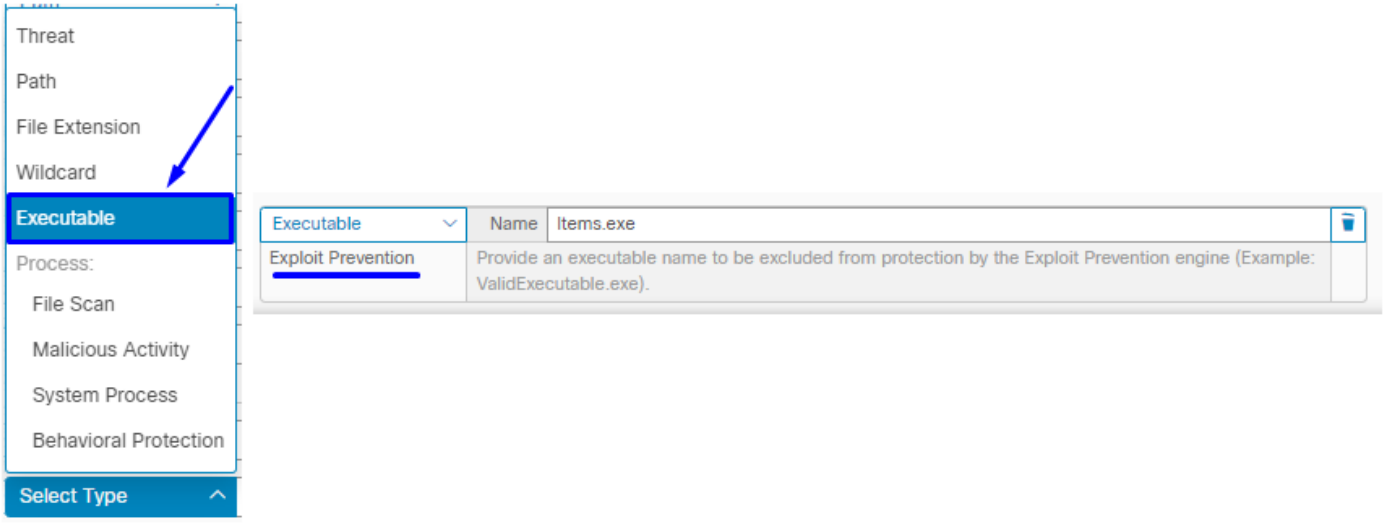
一旦识别了检测并且进程/可执行文件被您的环境信任和知道，就可以将其作为排除项进行添加。以防止连接器扫描它。

可执行排除项仅适用于已启用漏洞保护（连接器版本6.0.5及更高版本）的连接器。可执行排除用于从漏洞防御引擎中排除某些可执行文件。

> **注意**：不支持通配符和exe以外的扩展名。

您可以检查受保护进程的列表并从Exploit Prevention引擎中排除任何，您需要在application exclusion字段中指定其可执行文件名。您还可以从引擎中排除任何应用。可执行文件例外项需要完全匹配**name.exe**格式的可执行文件名称，如图所示。

> **注意**：将排除项应用到连接器后，需要重新启动从漏洞防御排除项中排除的任何可执行文件。如果禁用Exploit Prevention，则需要重新启动任何处于活动状态的受保护进程。




**注意**：确保将排除集添加到应用于受影响连接器的策略中。

最后，您可以监控行为。

如果漏洞防御检测仍然存在，请联系TAC支持以执行更深入的分析。您可以在此处找到所需信息：

- 漏洞防御事件的截图
- 设备轨迹和事件详细信息的截图
- 受影响的应用程序/进程的SHA256
- 禁用漏洞防御后是否会出现此问题？
- 禁用安全终端连接器服务时是否会出现此问题？
- 终端是否有任何其他安全或防病毒软件？
- 受影响的应用程序是什么？描述其功能
- 当问题发生时，启用调试模式的诊断文件（调试捆绑包日志）（在本文中，您可以找到如何收集诊断文件）

# 相关信息

- 安全终端用户指南
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。