對安全端點中的漏洞攻擊防禦進行故障排除

目錄

簡介

本文檔介紹安全終端控制檯中防漏洞攻擊引擎的配置以及如何執行基本分析。

必要條件

需求

思科建議您瞭解這些主題。

- 對安全終端控制檯的管理員訪問許可權
- 安全終端聯結器
- 已啟用防攻擊功能

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- 聯結器版本7.3.15或更高版本
- Windows 10 1709及更高版本或Windows Server 2016 1709及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔中介紹的步驟有助於瞭解如何根據在控制檯中觸發的事件，執行基本分析，並在您知道該過

程並在您的環境中使用該過程的情況下，建議您使用Exploit Prevention排除項。

利用漏洞防護引擎能夠保護您的終端免受惡意軟體常用的記憶體注入攻擊以及其他針對未修補軟體漏洞的零日攻擊。當檢測到對受保護進程的攻擊時，它會阻止並生成事件，但不會將其隔離。

受保護的進程

Exploit Prevention引擎可保護這些32位和64位（安全終端Windows聯結器6.2.1及更高版本）進程及其子進程：

- Microsoft Excel應用程式
- Microsoft Word應用程式
- Microsoft PowerPoint應用程式
- Microsoft Outlook應用程式
- Internet Explorer瀏覽器
- Mozilla Firefox瀏覽器
- Google Chrome瀏覽器
- Microsoft Skype應用程式
- TeamViewer應用程式
- VLC媒體播放器應用程式
- Microsoft Windows指令碼主機
- Microsoft Powershell應用程式
- Adobe Acrobat Reader應用程式
- Microsoft Register Server
- Microsoft任務計畫程式引擎
- Microsoft運行DLL命令
- Microsoft HTML應用程式主機
- Windows指令碼主機
- Microsoft程式集註冊工具
- 縮放
- Slack
- 思科Webex Teams
- Microsoft Teams

排除的進程

這些進程被從防漏洞攻擊引擎中排除（未被監控），原因是存在相容性問題：

- McAfee DLP服務
- McAfee Endpoint Security Utility

防漏洞攻擊版本5（聯結器版本7.5.1及更高版本）

安全端點Windows聯結器7.5.1包含漏洞防護的重要更新。此版本中的新功能包括：

- 保護網路驅動器：自動保護從網路驅動器運行的進程免受勒索軟體等威脅的侵擾
- 保護遠端進程：自動保護在使用域身份驗證使用者(admin)的受保護電腦上遠端運行的進程
- 通過rundll32的AppControl bypass:停止允許運行解釋命令的巧盡心思構建的rundll32命令列

- UAC旁路：阻止由惡意進程提升許可權，可防止Windows使用者帳戶控制機制繞過
- 瀏覽器/Mimikatz電子倉庫憑證：如果啟用，Exploit Prevention可防止Microsoft Internet Explorer和Edge瀏覽器中的憑據失竊
- 卷影副本刪除：跟蹤卷影副本的刪除並擷取Microsoft卷影復制服務(vssvc.exe)中的COM API
- SAM雜湊：防止Mimikatz竊取的SAM雜湊憑證，攔截嘗試列舉和解密登錄檔配置單元Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users中的所有SAM哈希

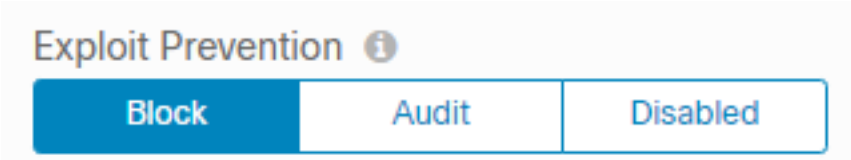
- 保護已執行的進程：如果運行進程在防漏洞攻擊例項之前已啟動(explorer.exe、lsass.exe、spoolsv.exe、winlogon.exe)，則插入這些進程

在策略中啟用Exploit Prevention時，預設情況下將啟用所有這些功能。

組態

若要啟用防漏洞攻擊引擎，請在策略中導航到**Modes and Engine**，然後選擇Audit mode、Block mode或Disabled模式，如下圖所示。

> **附註**：稽核模式僅在安全終結點Windows聯結器7.3.1及更高版本上可用。早期版本的聯結器將稽核模式視為與塊模式相同。

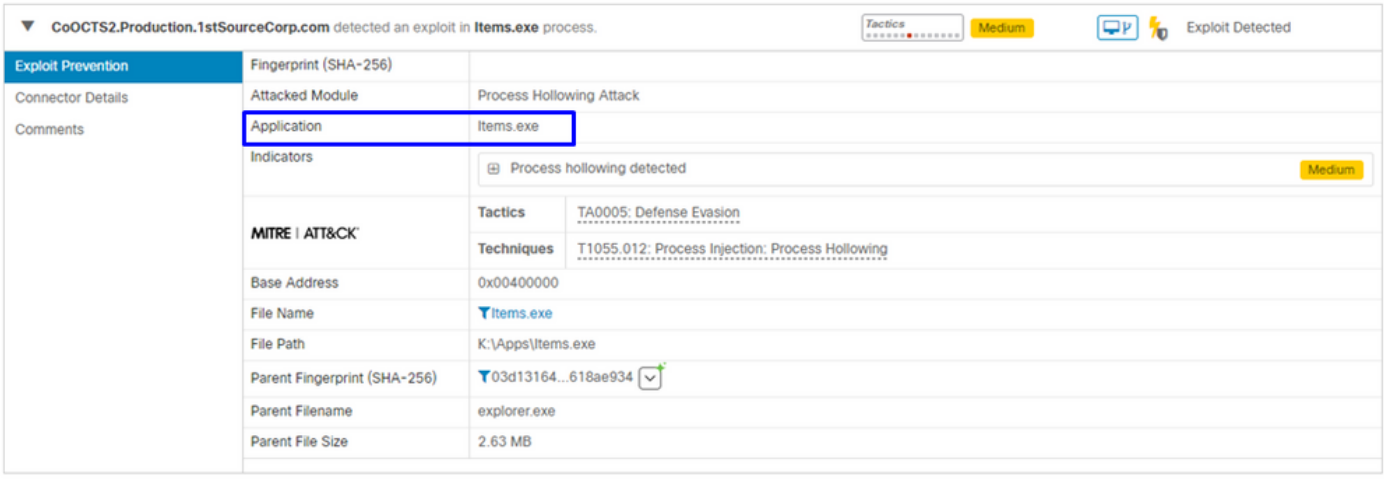


> **附註**：在Windows 7和Windows Server 2008 R2上，在安裝聯結器之前，需要應用Microsoft安全建議3033929的修補程式。

檢測

觸發檢測後，端點會顯示彈出通知，如下圖所示。

控制檯顯示「Exploit Prevention」事件，如圖所示。

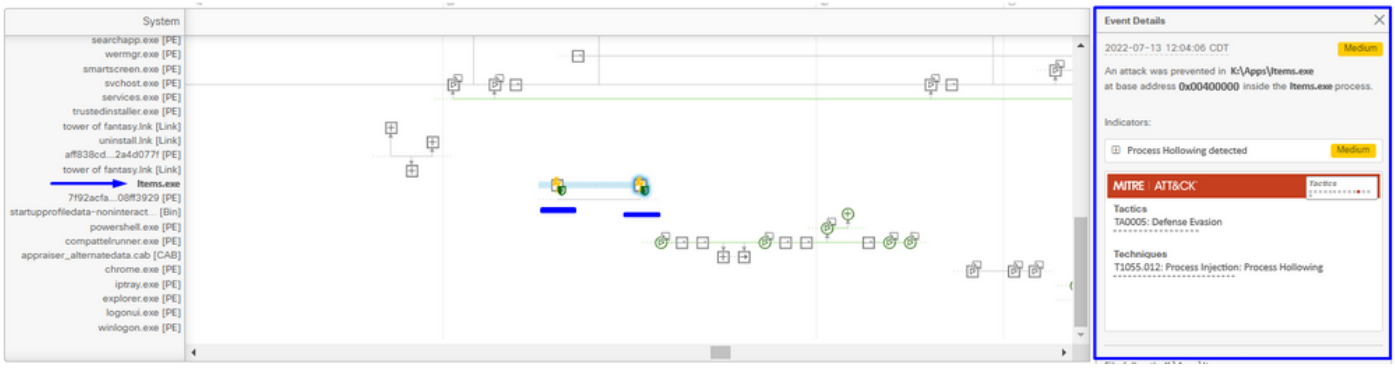


疑難排解

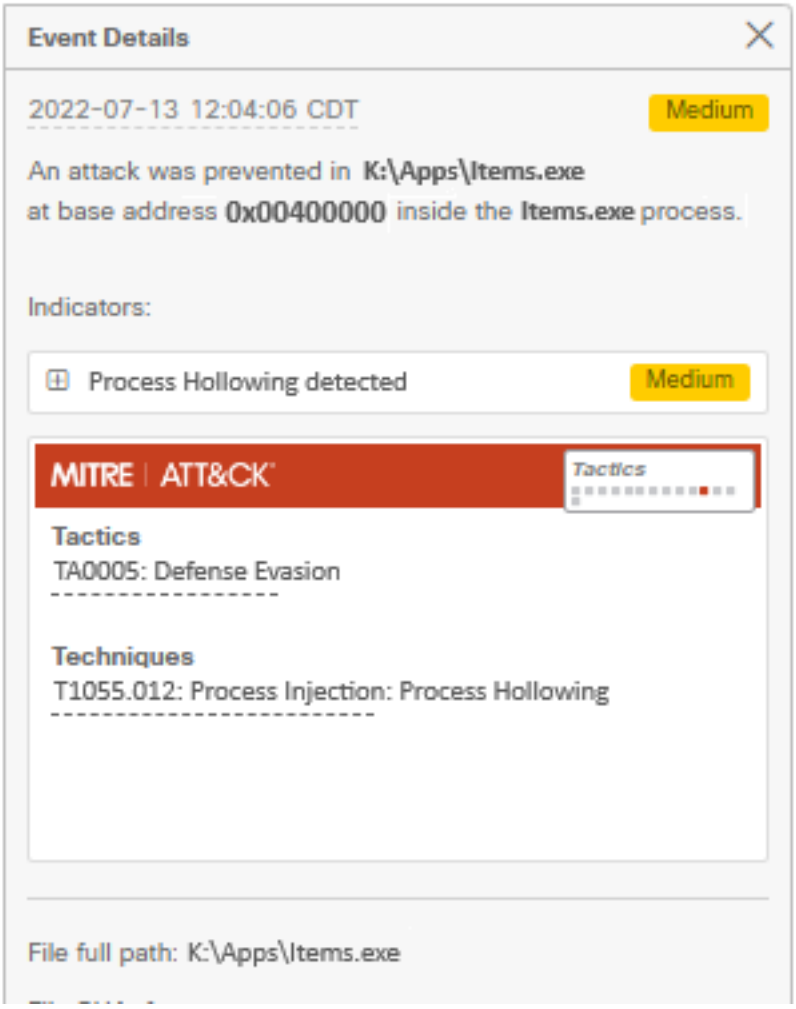
當控制檯中觸發漏洞防護事件時，識別檢測到的進程的方法是基於詳細資訊以提供對應用程式或進程運行時所發生事件的可視性，您可以導航到**Device Trajectory**。

步驟1。按一下Exploit Prevention事件中發生的**Device Trajectory**圖示，如下圖所示。

步驟2.在Device Trajectory的時間表中找到Exploit Prevention圖示，以檢視**Event Details**部分，如下圖所示。



步驟3.確定事件的詳細資訊，並評估您的環境中是否信任或瞭解該流程或應用程式。



誤報檢測

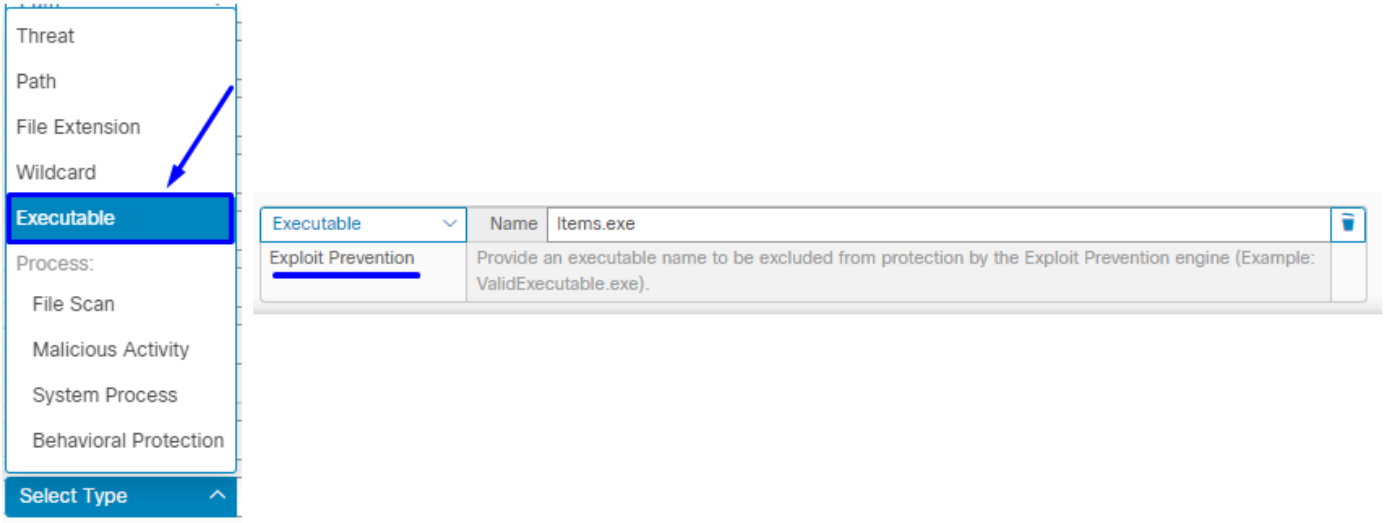
一旦識別出該檢測，並且您的環境信任並知道該進程/執行檔，則可以將其新增為排除。以防止聯結器掃描到該聯結器。

執行檔排除項僅適用於已啟用利用漏洞防護（聯結器版本6.0.5及更高版本）的聯結器。執行檔排除用於從漏洞防護引擎中排除某些執行檔。

> **注意**：不支援萬用字元和exe以外的副檔名。

您可以檢查受保護進程的清單並從防漏洞攻擊引擎中排除任何進程，您需要在應用程式排除欄位中指定其執行檔名。您還可以從引擎中排除任何應用程式。執行檔排除項需要與執行檔名稱完全匹配，格式為**name.exe**，如圖所示。

> **附註**：從防漏洞攻擊中排除的任何執行檔都需要在將排除項應用到聯結器後重新啟動。如果禁用Exploit Prevention，則需要重新啟動任何處於活動狀態的受保護進程。



附註：確保將排除集新增到應用於受影響聯結器的策略中。

最後，您可以監視行為。

如果防漏洞檢測仍然存在，請聯絡TAC支援以執行更深入的分析。您可以在此處找到所需的資訊：

- Exploit Prevention事件的截圖
- 裝置軌跡和事件詳細資訊的螢幕截圖
- 受影響的應用程式/進程的SHA256
- 禁用了防漏洞攻擊後，是否會出現問題？
- 禁用安全終結點聯結器服務時是否出現問題？
- 終端是否有任何其他安全或防病毒軟體？
- 受影響的應用程式是什麼？描述其功能
- 發生問題時啟用調試模式的診斷檔案（調試捆綁包日誌）（在本文中，您可以找到如何收集診斷檔案）

相關資訊

- 安全端點使用手冊
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。