Troubleshoot Exploit Prevention in Secure Endpoint

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Protected Processes](#)
[Excluded Processes](#)
[Exploit Prevention version 5 (Connector version 7.5.1 and later)](#)
[Configuration](#)
[Detection](#)
[Troubleshoot](#)
[False Positive Detection](#)
[Related Information](#)

Introduction

This document describes the configuration of the Exploit Prevention engine in the Secure Endpoint console and how to perform basic analysis.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics.

- Admin access to Secure Endpoint console
- Secure Endpoint Connector
- Exploit Prevention feature enabled

Components Used

The information in this document is based on these software and hardware versions.

- Connector version 7.3.15 or later
- Windows 10 version 1709 and later or Windows Server 2016 version 1709 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The procedure described in this document is helpful on how to perform a basic analysis based on the events, triggered in the console and suggests you Exploit Prevention exclusions in case you know the process and use it in your environment.

The Exploit Prevention engine provides the ability to defend your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software vulnerabilities. When it detects an attack against a protected process it is blocked and generates an event but it is not quarantined.

Protected Processes

The Exploit Prevention engine protects these 32-bit and 64-bit (Secure Endpoint Windows connector version 6.2.1 and higher) processes and their child processes:

- Microsoft Excel Application
- Microsoft Word Application
- Microsoft PowerPoint Application
- Microsoft Outlook Application
- Internet Explorer Browser
- Mozilla Firefox Browser
- Google Chrome Browser
- Microsoft Skype Application
- TeamViewer Application
- VLC Media player Application
- Microsoft Windows Script Host
- Microsoft Powershell Application
- Adobe Acrobat Reader Application
- Microsoft Register Server
- Microsoft Task Scheduler Engine
- Microsoft Run DLL Command
- Microsoft HTML Application Host
- Windows Script Host
- Microsoft Assembly Registration Tool
- Zoom
- Slack
- Cisco Webex Teams
- Microsoft Teams

Excluded Processes

These processes are excluded (not monitored) from the Exploit Prevention engine because of compatibility issues:

- McAfee DLP Service
- McAfee Endpoint Security Utility

Exploit Prevention version 5 (Connector version 7.5.1 and later)

Secure Endpoint Windows connector 7.5.1 includes a significant update to Exploit Prevention. New features in this version include:

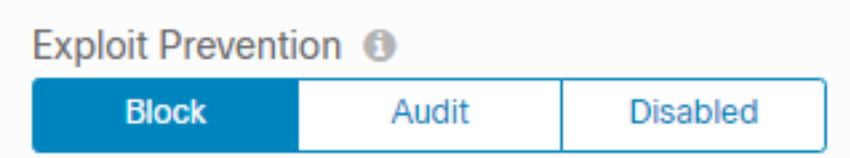
- Protect network drives: Automatically protects processes that run from network drives against threats like ransomware
- Protect remote processes: Automatically protects processes that run remotely on protected computers that use a domain authenticated user (admin)
- AppControl bypass through rundll32: Stops specially crafted rundll32 command lines that allow to run interpreted commands
- UAC bypass: Blocks privilege escalation by malicious processes, it prevents Windows User Account Control mechanism bypasses
- Browser/Mimikatz vaults credential: If enabled, Exploit Prevention protects against credential theft in Microsoft Internet Explorer and Edge browsers
- Shadow copy deletion: Traces the deletion of shadow copies, and intercepts the COM API in the Microsoft Volume Shadow Copy Service (vssvc.exe)
- SAM hashes: Protects against SAM hash credential theft by Mimikatz, intercepts attempts to enumerate and decrypt all the SAM hashes in the registry hive **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**
- Protect processes executed: Inject into processes that run, if those have started before the Exploit Prevention instance (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

These features are all enabled by default when Exploit Prevention is enabled in policy.

Configuration

In order to enable the Exploit Prevention engine, navigate to **Modes and Engines** in your policy and select Audit mode, Block mode, or Disabled mode, as shown in the image.

> **Note**: Audit mode is only available on Secure Endpoint Windows connector 7.3.1 and later. Earlier versions of the connector treat audit mode the same as block mode.

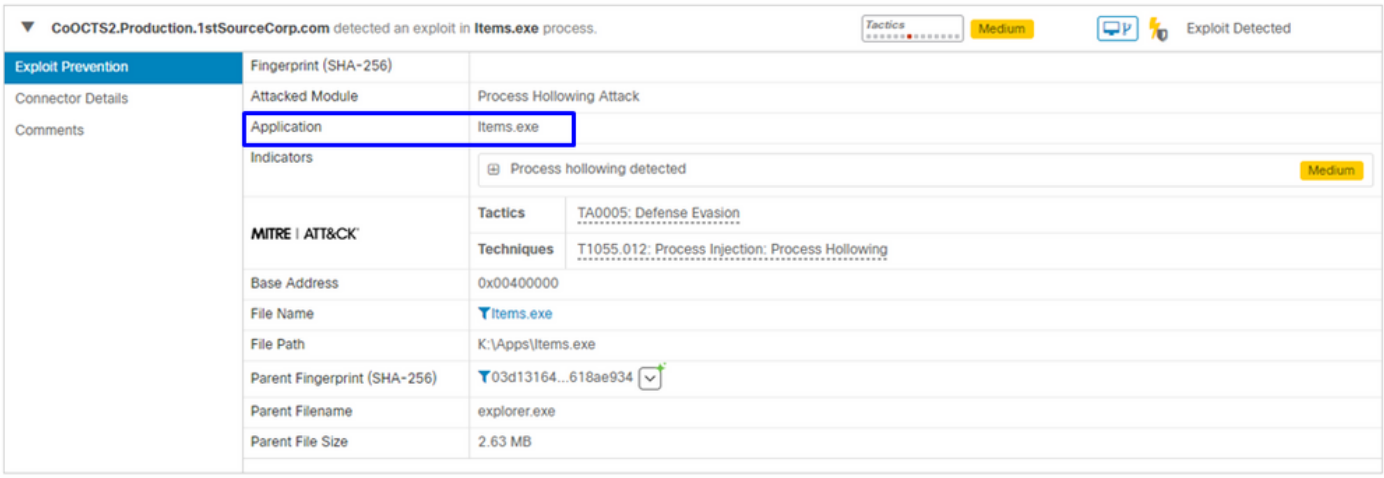


> **Note**: On Windows 7 and Windows Server 2008 R2 you need to apply the patch for Microsoft Security Advisory 3033929 before you install the connector.

Detection

Once the detection is triggered, a pop-up notification is displayed on the endpoint, as shown in the image.

The console displays an Exploit Prevention event, as shown in the image.

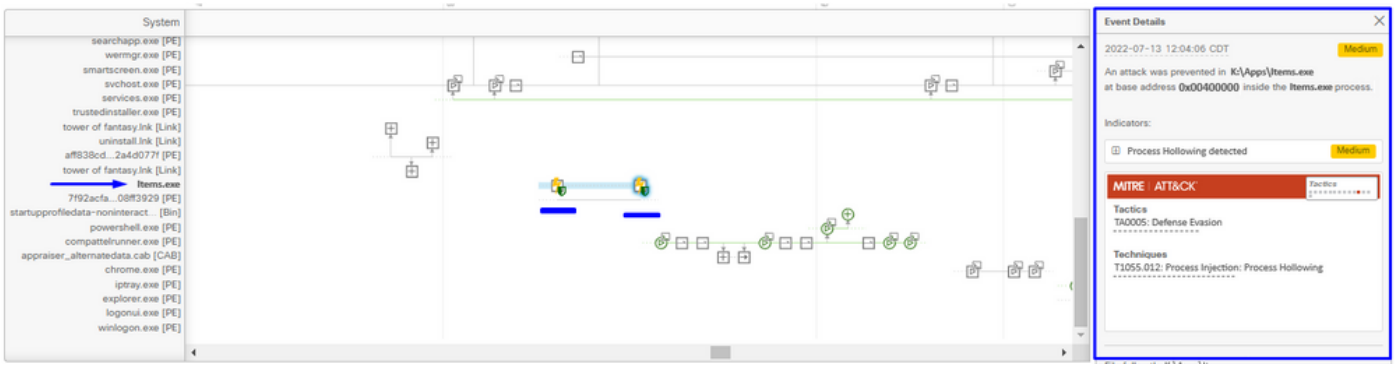


Troubleshoot

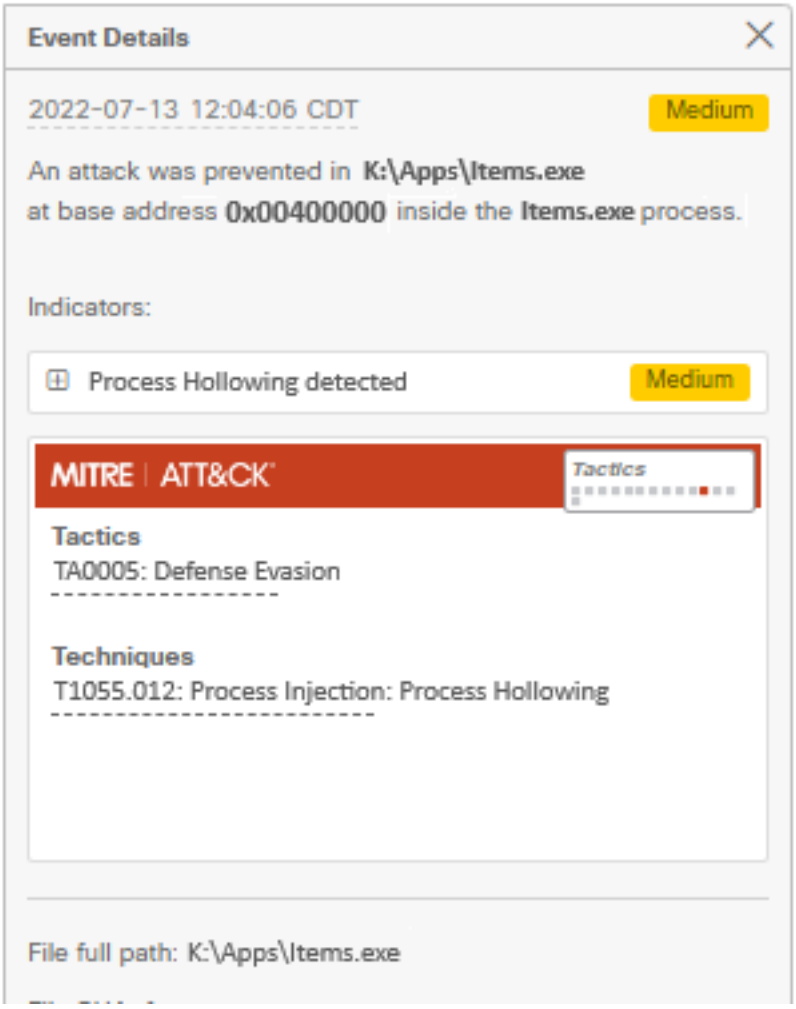
When an Exploit Prevention event is triggered in the console, a way to identify the process detected is based on the details to provide you visibility into the events that occurred while the application or process ran, you can navigate to the **Device Trajectory**.

Step 1. Click on the **Device Trajectory** icon that appears in the Exploit Prevention event, as shown in the image.

Step 2. Find the Exploit Prevention icon in the timeline of the Device Trajectory in order to see the **Event Details** section, as shown in the image.



Step 3. Identify the details of the event, and evaluate if the process or application is trusted/known in your environment.



False Positive Detection

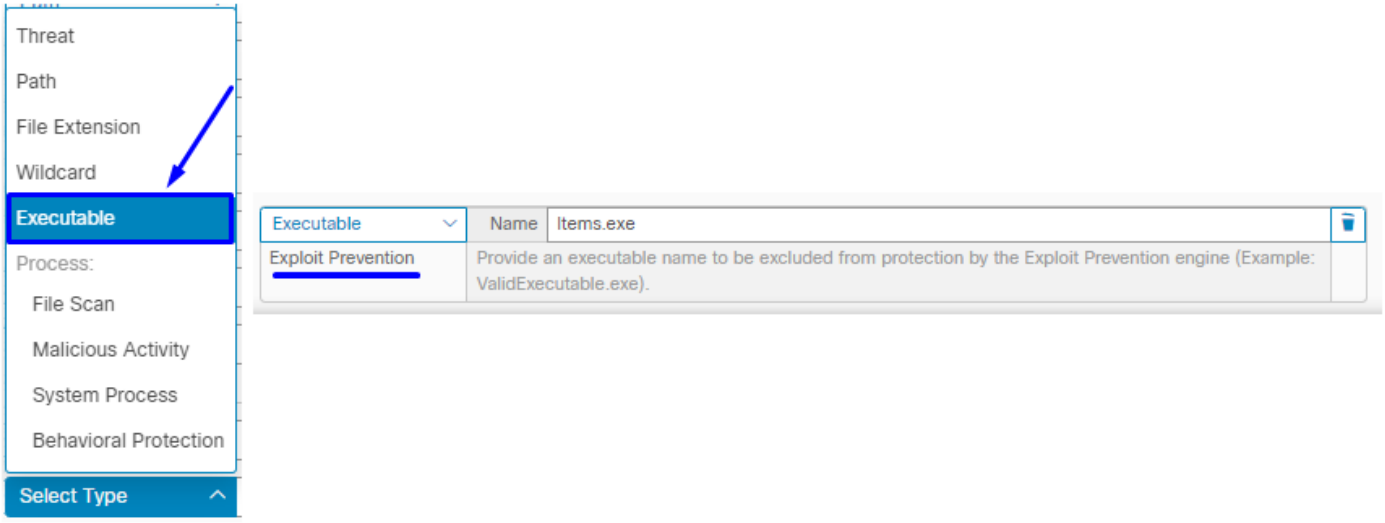
Once the detection is identified and if the process/executable is trusted and known by your environment, it can be added as an exclusion. In order to prevent the connector scans to it.

Executable exclusions only apply to connectors with Exploit Prevention (Connector version 6.0.5 and later) enabled. An executable exclusion is used to exclude certain executables from the Exploit Prevention engine.

> **Caution**: Wildcards and extensions other than exe are not supported.

You can check the list of Protected Processes and exclude any from the Exploit Prevention engine, you need to specify its executable name in the application exclusion field. You can also exclude any applications from the engine. Executable exclusions need to match the executable name exactly in the format **name.exe**, as shown in the image.

> **Note**: Any executables you exclude from Exploit Prevention need to be restarted after the exclusion is applied to the connector. And if you disable Exploit Prevention you need to restart any of the protected processes that were active.



Note: Ensure the exclusion set is added to the policy applied to the affected connector.

Finally, you can monitor the behavior.

In case the Exploit Prevention detection persists, please contact TAC support in order to perform a deeper analysis. Here you can find the information required:

- Screenshot of the Exploit Prevention event
- Screenshot of the Device Trajectory and Event Details
- SHA256 of the affected application/process
- Does the issue occur with Exploit Prevention disabled?
- Does the issue occur with the Secure Endpoint connector service disabled?
- Does the endpoint have any other Security or Antivirus software?
- What is the affected application? Describe its function
- Diagnostic file (Debug bundle logs) with Debug mode enabled when the issue occurs (in this article you can find how to collect the Diagnostic file)

Related Information

- Secure Endpoint User Guide
- Technical Support & Documentation - Cisco Systems