Solución de problemas de prevención de vulnerabilidades en terminales seguros

Contenido

Introducción

Este documento describe la configuración del motor de prevención de vulnerabilidades en la consola de Secure Endpoint y cómo realizar análisis básicos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- Acceso de administrador a la consola de Secure Endpoint
- Conector de terminal seguro
- Función de prevención de vulnerabilidades activada

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Versión del conector 7.3.15 o posterior
- Windows 10 versión 1709 y posterior o Windows Server 2016 versión 1709 y posterior

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El procedimiento descrito en este documento es útil para realizar un análisis básico basado en los eventos, activados en la consola y sugiere exclusiones de prevención de exploits en caso de que conozca el proceso y lo utilice en su entorno.

El motor de prevención de vulnerabilidades ofrece la posibilidad de proteger los terminales frente a los ataques de inyección de memoria utilizados habitualmente por malware y otros ataques de día cero contra vulnerabilidades de software sin parches. Cuando detecta un ataque contra un proceso protegido, se bloquea y genera un evento, pero no se pone en cuarentena.

Procesos protegidos

El motor de prevención de vulnerabilidades protege estos procesos de 32 bits y 64 bits (conector Secure Endpoint Windows versión 6.2.1 y posteriores) y sus procesos secundarios:

- Aplicación de Microsoft Excel
- Aplicación de Microsoft Word
- Aplicación de Microsoft PowerPoint
- Aplicación de Microsoft Outlook
- Explorador de Internet Explorer
- Navegador Mozilla Firefox
- Navegador Google Chrome
- Aplicación Microsoft Skype
- Aplicación TeamViewer
- Aplicación de reproductor multimedia VLC
- Microsoft Windows Script Host
- Aplicación Microsoft Powershell
- Aplicación Adobe Acrobat Reader
- Microsoft Register Server
- Microsoft Task Scheduler Engine
- Comando Microsoft Run DLL
- Host de aplicación HTML de Microsoft
- Windows Script Host
- Herramienta Registro de ensamblados de Microsoft
- ZOOM
- Holgura
- Equipos de Cisco Webex
- Equipos de Microsoft

Procesos excluidos

Estos procesos se excluyen (no se supervisan) del motor de prevención de vulnerabilidades debido a problemas de compatibilidad:

- Servicio DLP de McAfee
- Utilidad McAfee Endpoint Security

Prevención de vulnerabilidades versión 5 (versión del conector 7.5.1 y posteriores)

El conector de Windows de terminal seguro 7.5.1 incluye una actualización significativa de la prevención de vulnerabilidades. Las nuevas funciones de esta versión incluyen:

- Proteja las unidades de red: Protege automáticamente los procesos que se ejecutan desde unidades de red frente a amenazas como el ransomware
- Proteja los procesos remotos: Protege automáticamente los procesos que se ejecutan de forma remota en equipos protegidos que utilizan un dominio de usuario autenticado (admin)
- Omisión de AppControl a través de rundll32: Detiene las líneas de comandos rundll32 especialmente diseñadas que permiten ejecutar comandos interpretados
- Omisión de UAC: Bloquea la ampliación de privilegios por parte de procesos maliciosos, evita que el mecanismo de control de cuentas de usuario de Windows pase por alto
- Credencial de Browser/Mimikatz vaults: Si está activada, la prevención de vulnerabilidades protege contra el robo de credenciales en Microsoft Internet Explorer y los navegadores periféricos
- Eliminación de instantáneas: Realiza un seguimiento de la eliminación de instantáneas e intercepta la API COM en el Servicio de instantáneas de volumen de Microsoft (vssvc.exe)
- Hashes SAM: Protege contra el robo de credenciales de hash SAM por parte de Mimikatz, intercepta los intentos de enumerar y descifrar todos los hash SAM del subárbol del Registro **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**

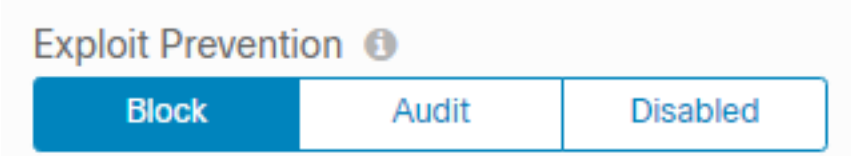
- Proteger procesos ejecutados: Inyectar en procesos que se ejecuten, si se han iniciado antes de la instancia de Prevención de exploits (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Todas estas funciones se activan de forma predeterminada cuando la prevención de vulnerabilidades está activada en la directiva.

Configuración

Para habilitar el motor de prevención de exploits, navegue hasta **Modos y motores** en su política y seleccione el modo de auditoría, el modo de bloqueo o el modo inhabilitado, como se muestra en la imagen.

> **Nota:** El modo de auditoría sólo está disponible en el conector Secure Endpoint Windows 7.3.1 y versiones posteriores. Las versiones anteriores del conector tratan el modo auditoría igual que el modo de bloqueo.

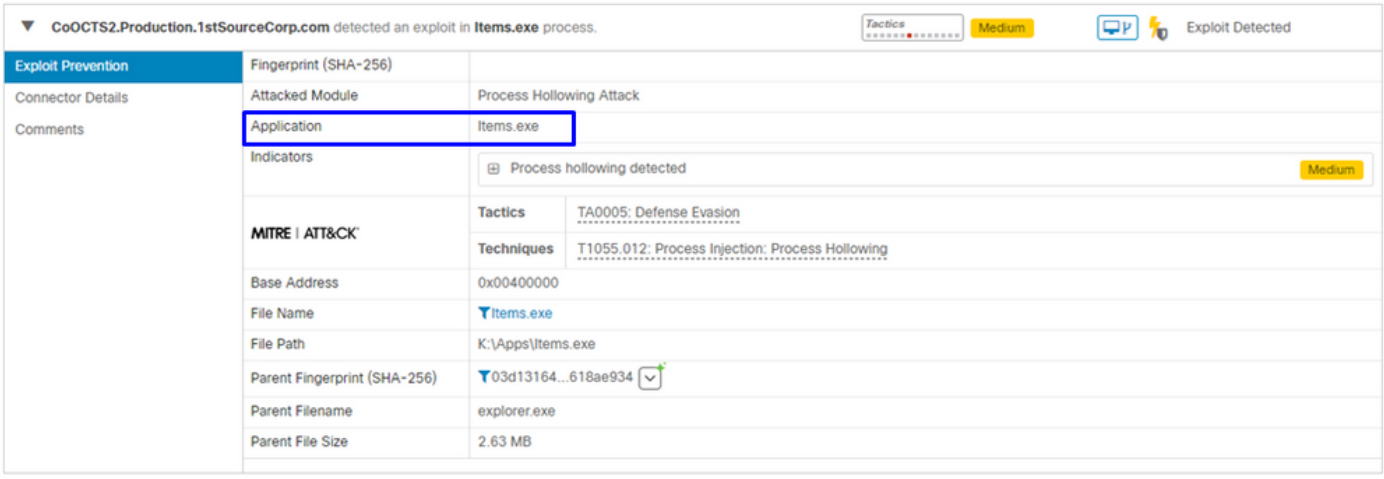


> **Nota:** En Windows 7 y Windows Server 2008 R2, debe aplicar la revisión de Microsoft Security Advisory 303929 antes de instalar el conector.

Detección

Una vez activada la detección, se muestra una notificación emergente en el terminal, como se muestra en la imagen.

La consola muestra un evento de prevención de exploits, como se muestra en la imagen.

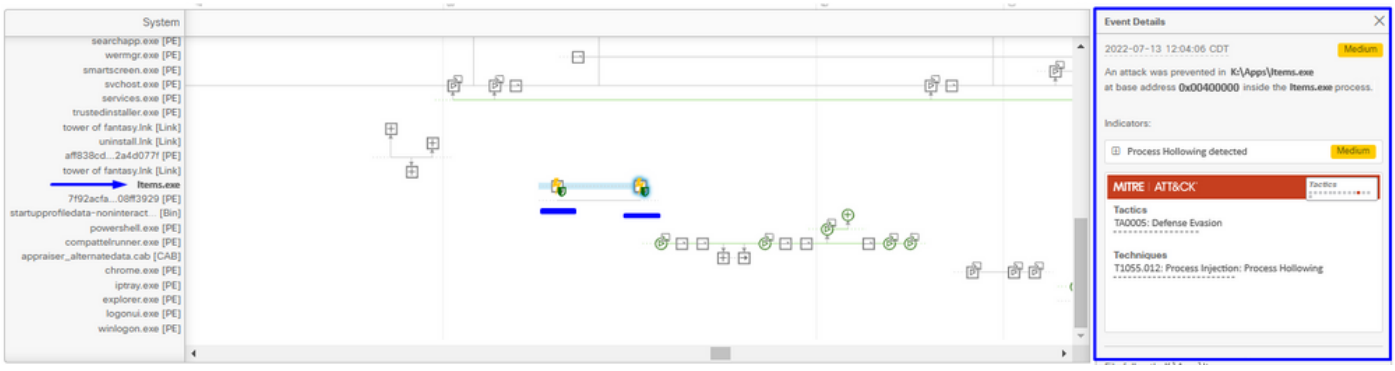


Troubleshoot

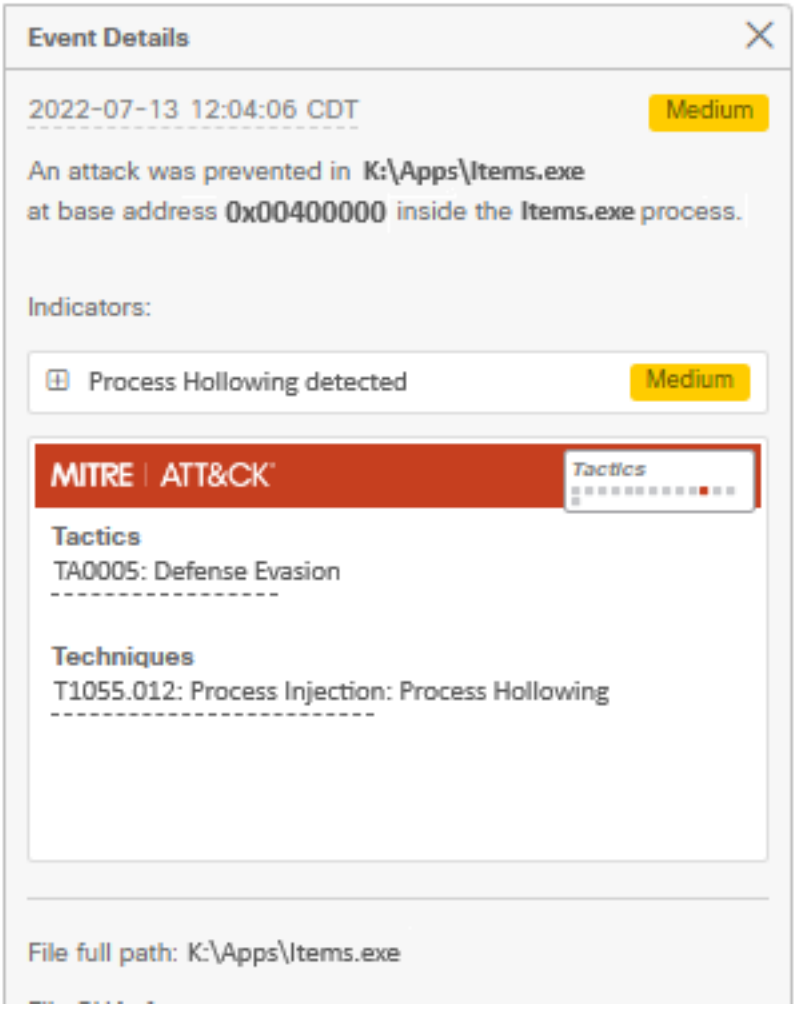
Cuando se activa un evento de prevención de vulnerabilidades en la consola, se puede identificar el proceso detectado en función de los detalles para proporcionar visibilidad de los eventos que se han producido mientras se ejecutaba la aplicación o el proceso. Para ello, se puede navegar hasta la **trayectoria del dispositivo**.

Paso 1. Haga clic en el icono **Trayectoria del dispositivo** que aparece en el evento de prevención de exploits, como se muestra en la imagen.

Paso 2. Busque el icono de prevención de exploits en la línea de tiempo de la trayectoria del dispositivo para ver la sección **Detalles del evento**, como se muestra en la imagen.



Paso 3. Identifique los detalles del evento y evalúe si el proceso o la aplicación es de confianza o conocido en su entorno.



Detección de falsos positivos

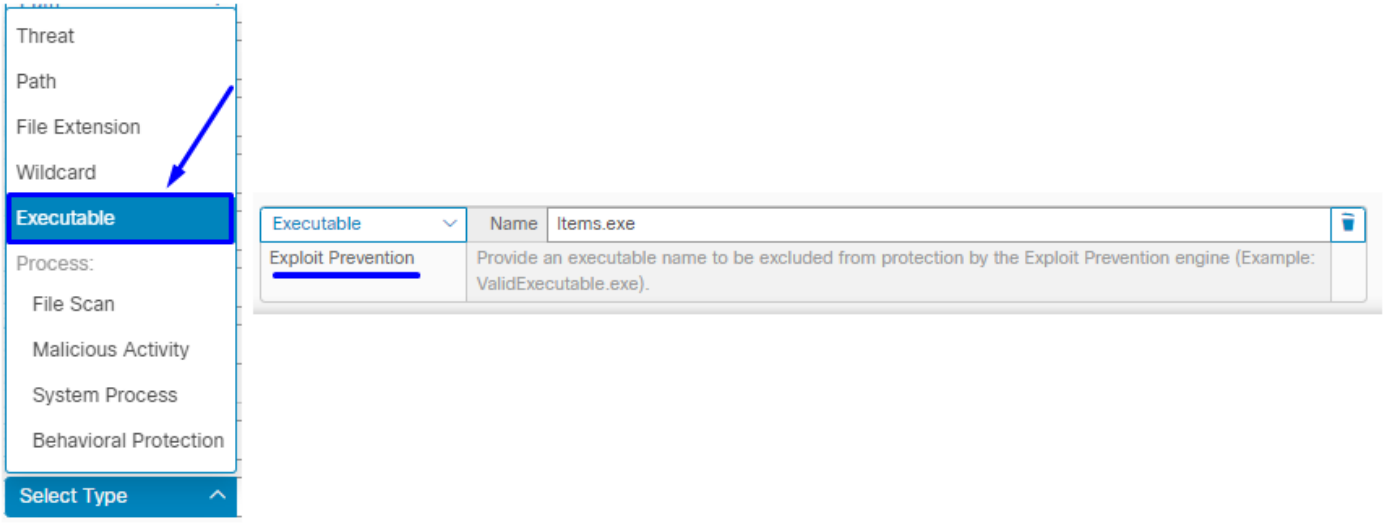
Una vez identificada la detección y si el entorno confía en el proceso/ejecutable y lo conoce, se puede agregar como exclusión. Para evitar que el conector escanee.

Las exclusiones ejecutables sólo se aplican a los conectores con la prevención de vulnerabilidades (Connector version 6.0.5 y posterior) habilitada. La exclusión de ejecutables se utiliza para excluir determinados ejecutables del motor de prevención de vulnerabilidades.

> **Precaución**: no se admiten comodines ni extensiones que no sean exe.

Puede comprobar la lista de procesos protegidos y excluir cualquier elemento del motor de prevención de exploits; debe especificar su nombre de ejecutable en el campo de exclusión de la aplicación. También puede excluir cualquier aplicación del motor. Las exclusiones ejecutables deben coincidir exactamente con el nombre del ejecutable en el formato **name.exe**, como se muestra en la imagen.

> **Nota:** Los ejecutables que excluya de la prevención de exploits deben reiniciarse después de aplicar la exclusión al conector. Y si desactiva la prevención de vulnerabilidades, debe reiniciar cualquiera de los procesos protegidos que estaban activos.



> **Nota:** Asegúrese de agregar el conjunto de exclusión a la política aplicada al conector afectado.

Por último, puede supervisar el comportamiento.

En caso de que la detección de la prevención de vulnerabilidades persista, póngase en contacto con el soporte técnico del TAC para realizar un análisis más detallado. Aquí puede encontrar la información requerida:

- Captura de pantalla del evento de prevención de vulnerabilidades
- Captura de pantalla de la trayectoria del dispositivo y detalles del evento
- SHA256 de la solicitud o proceso afectado
- ¿Se produce el problema con la prevención de vulnerabilidades desactivada?
- ¿Ocurre el problema con el servicio de conector de terminal seguro deshabilitado?
- ¿Tiene el terminal algún otro software de seguridad o antivirus?
- ¿Cuál es la aplicación afectada? Describir su función
- Archivo de diagnóstico (registros de paquetes de depuración) con el modo de depuración habilitado cuando se produce el problema (en este artículo se puede encontrar cómo recopilar el archivo de diagnóstico)

Información Relacionada

- Guía del usuario de terminales seguros
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).