Dépannage de la prévention des exploits dans Secure Endpoint

Contenu

Introduction

Ce document décrit la configuration du moteur de prévention des exploits dans la console Secure Endpoint et comment effectuer une analyse de base.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- Accès administrateur à la console Secure Endpoint
- Connecteur de terminal sécurisé
- Fonction de prévention des exploits activée

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Connecteur version 7.3.15 ou ultérieure
- Windows 10 version 1709 et ultérieure ou Windows Server 2016 version 1709 et ultérieure

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

La procédure décrite dans ce document est utile pour effectuer une analyse de base basée sur les événements déclenchés dans la console et vous suggère d'exclure la prévention des exploits si vous connaissez le processus et l'utilisez dans votre environnement.

Le moteur de prévention des exploits offre la possibilité de protéger vos terminaux contre les attaques par injection de mémoire couramment utilisées par les programmes malveillants et d'autres attaques zero-day sur des vulnérabilités logicielles non corrigées. Lorsqu'il détecte une attaque contre un processus protégé, il est bloqué et génère un événement, mais il n'est pas mis en quarantaine.

Processus protégés

Le moteur de prévention des exploits protège ces processus 32 bits et 64 bits (connecteur Windows Secure Endpoint version 6.2.1 et ultérieure) et leurs processus enfants :

- Application Microsoft Excel
- Application Microsoft Word
- Application Microsoft PowerPoint
- Application Microsoft Outlook
- Navigateur Internet Explorer
- Navigateur Mozilla Firefox
- Navigateur Google Chrome
- Application Microsoft Skype
- Application TeamViewer
- Application de lecteur multimédia VLC
- Microsoft Windows Script Host
- Application Microsoft Powershell
- Application Adobe Acrobat Reader
- Serveur d'enregistrement Microsoft
- Moteur du Planificateur de tâches Microsoft
- Commande Exécuter la DLL Microsoft
- Hôte d'application Microsoft HTML
- Windows Script Host
- Outil Microsoft Assembly Registration Tool
- Zoom
- Mou
- Équipes Cisco Webex
- Microsoft Teams

Processus exclus

Ces processus sont exclus (non surveillés) du moteur de prévention des exploits en raison de problèmes de compatibilité :

- Service McAfee DLP
- Utilitaire McAfee Endpoint Security

Prévention des exploits version 5 (Connecteur version 7.5.1 et ultérieure)

Le connecteur Windows 7.5.1 Secure Endpoint inclut une mise à jour significative de la prévention des exploits. Les nouvelles fonctionnalités de cette version incluent :

- Protection des lecteurs réseau : Protège automatiquement les processus qui s'exécutent à partir des lecteurs réseau contre les menaces telles que les ransomwares
- Protéger les processus distants : Protège automatiquement les processus qui s'exécutent à distance sur les ordinateurs protégés qui utilisent un utilisateur authentifié par domaine (admin)
- Contournement AppControl via rundll32 : Arrête les lignes de commande rundll32 spécialement conçues pour permettre l'exécution de commandes interprétées
- Contournement UAC : Bloque l'escalade des privilèges par des processus malveillants, il empêche le mécanisme de contrôle de compte d'utilisateur Windows de contourner
- Informations d'identification du navigateur/coffre Mimikatz : Si cette option est activée, la prévention des exploits protège contre le vol d'informations d'identification dans Microsoft Internet Explorer et les navigateurs Edge
- Suppression du cliché instantané : Suit la suppression des clichés instantanés et intercepte l'API COM dans le service de cliché instantané des volumes Microsoft (vssvc.exe)
- Hachages SAM : Protège contre le vol des identifiants de hachage SAM par Mimikatz, intercepte les tentatives d'énumération et de déchiffrement de tous les hachages SAM dans la ruche de registre **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**

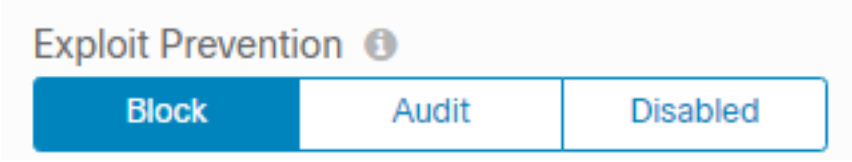
- Protéger les processus exécutés : Injecter dans les processus qui s'exécutent, si ceux-ci ont démarré avant l'instance de prévention des exploits (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Ces fonctionnalités sont toutes activées par défaut lorsque la prévention des exploits est activée dans la stratégie.

Configuration

Afin d'activer le moteur de prévention des exploits, accédez à **Modes et moteurs** dans votre stratégie et sélectionnez le mode Audit, le mode Block ou le mode Disabled, comme indiqué dans l'image.

> **Note**: Le mode Audit est uniquement disponible sur le connecteur Windows Secure Endpoint 7.3.1 et versions ultérieures. Les versions antérieures du connecteur traitent le mode audit de la même manière que le mode bloc.

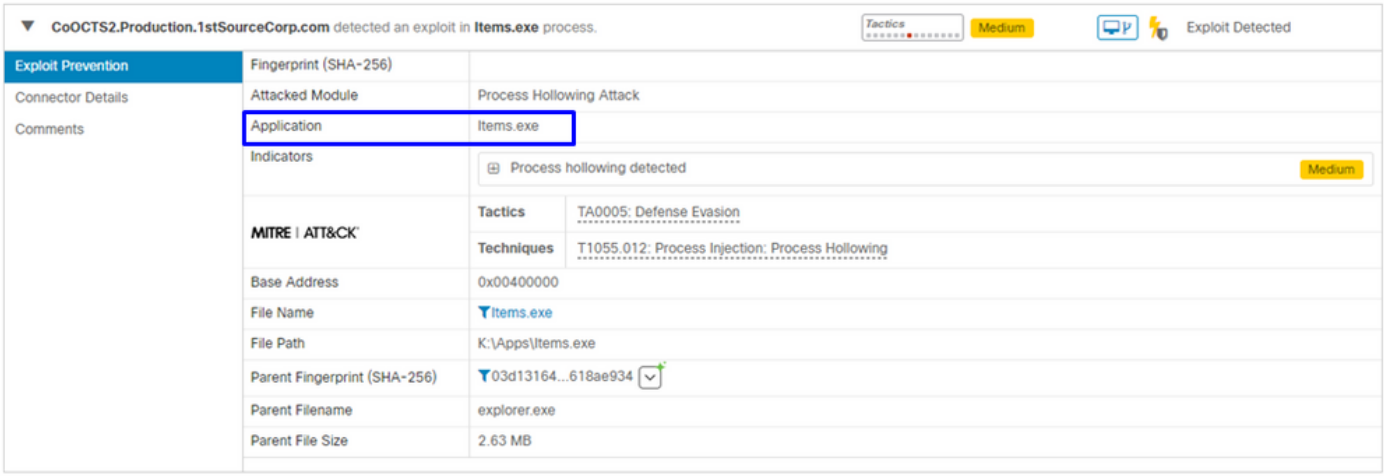


> **Note**: Sous Windows 7 et Windows Server 2008 R2, vous devez appliquer le correctif pour Microsoft Security Advisory 303929 avant d'installer le connecteur.

Détection

Une fois la détection déclenchée, une notification contextuelle s'affiche sur le terminal, comme illustré dans l'image.

La console affiche un événement de prévention des exploits, comme illustré dans l'image.

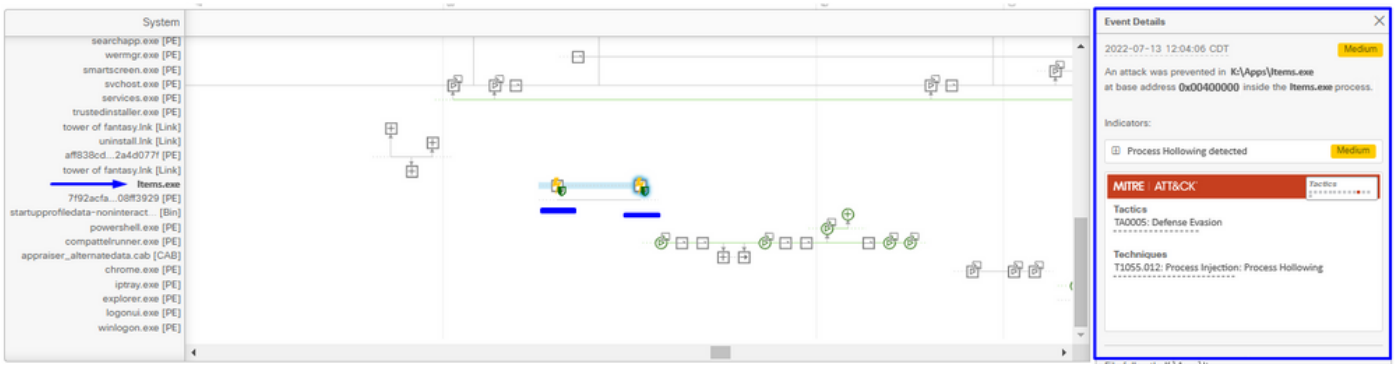


Dépannage

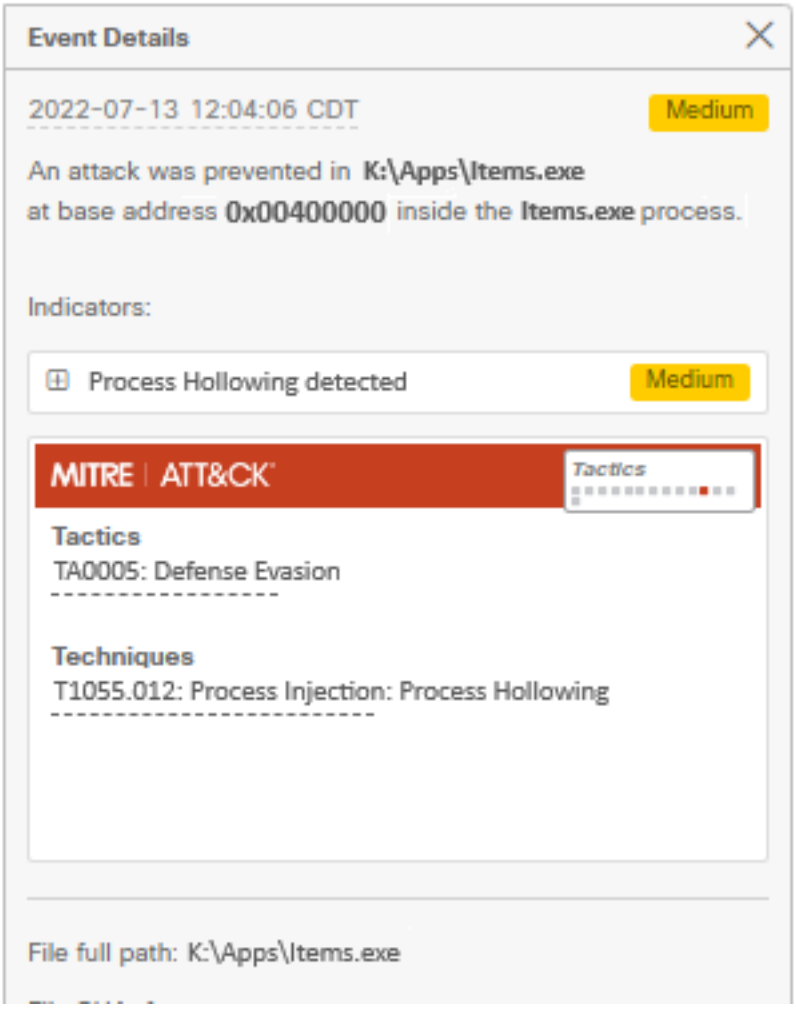
Lorsqu'un événement de prévention des exploits est déclenché dans la console, une méthode d'identification du processus détecté est basée sur les détails pour vous fournir une visibilité sur les événements qui se sont produits pendant l'exécution de l'application ou du processus. Vous pouvez accéder à la **trajectoire du périphérique**.

Étape 1. Cliquez sur l'icône **Device Trajectory** qui apparaît dans l'événement Exploit Prevention, comme illustré dans l'image.

Étape 2. Recherchez l'icône Prévention des exploits dans la chronologie de la trajectoire du périphérique afin de voir la section **Détails de l'événement**, comme illustré dans l'image.



Étape 3. Identifiez les détails de l'événement et évaluez si le processus ou l'application est approuvé/connu dans votre environnement.



Détection des faux positifs

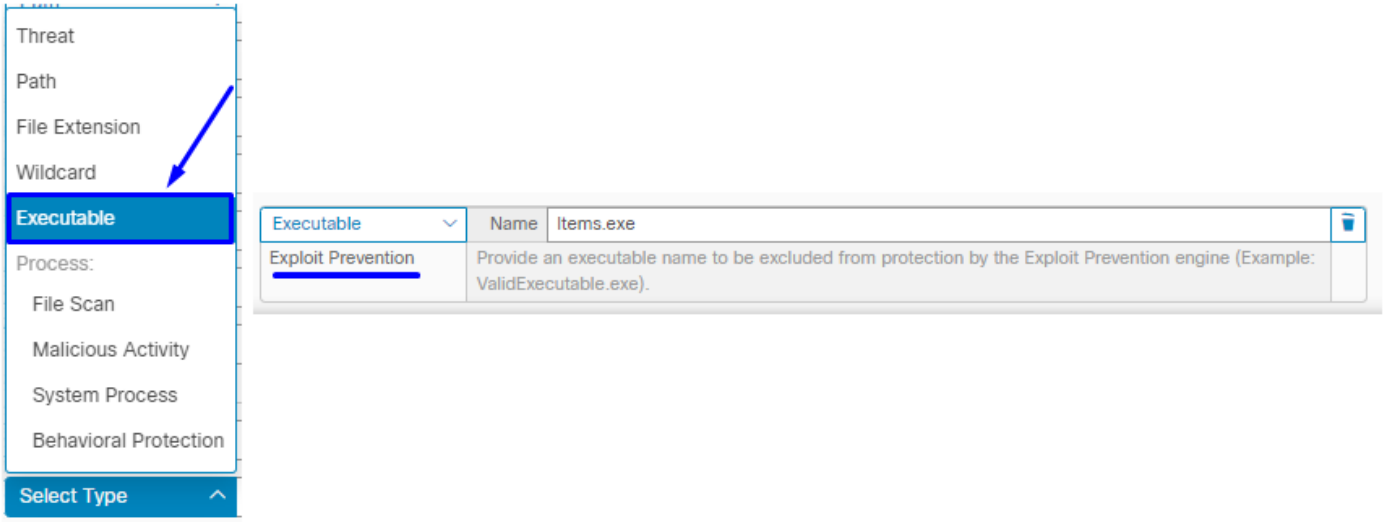
Une fois la détection identifiée et si le processus/exécutable est approuvé et connu par votre environnement, il peut être ajouté en tant qu'exclusion. Afin d'empêcher le connecteur scanne vers elle.

Les exclusions exécutables s'appliquent uniquement aux connecteurs pour lesquels la prévention des exploits (version 6.0.5 et ultérieure du connecteur) est activée. Une exclusion d'exécutable est utilisée pour exclure certains exécutables du moteur de prévention des exploits.

> **Attention** : les caractères génériques et les extensions autres que exe ne sont pas pris en charge.

Vous pouvez vérifier la liste des processus protégés et exclure tout processus du moteur de prévention des exploits. Vous devez spécifier son nom d'exécutable dans le champ d'exclusion d'application. Vous pouvez également exclure toutes les applications du moteur. Les exclusions d'exécutable doivent correspondre exactement au nom de l'exécutable au format **name.exe**, comme illustré dans l'image.

> **Note**: Tous les exécutables que vous excluez de la prévention des exploits doivent être redémarrés une fois l'exclusion appliquée au connecteur. Et si vous désactivez la prévention des exploits, vous devez redémarrer tous les processus protégés qui étaient actifs.



> **Note**: Assurez-vous que le jeu d'exclusions est ajouté à la stratégie appliquée au connecteur affecté.

Enfin, vous pouvez surveiller le comportement.

Si la détection de la prévention des exploits persiste, contactez le support du TAC afin d'effectuer une analyse plus approfondie. Vous trouverez ici les informations requises :

- Capture d'écran de l'événement Exploit Prevention
- Capture d'écran de la trajectoire du périphérique et détails des événements
- SHA256 de l'application/du processus affecté
- Le problème se produit-il lorsque la prévention des exploits est désactivée ?
- Le problème se produit-il lorsque le service Secure Endpoint Connector est désactivé ?
- Le terminal dispose-t-il d'un autre logiciel de sécurité ou antivirus ?
- Quelle est l'application concernée ? Décrire sa fonction
- Fichier de diagnostic (journaux de bundle de débogage) avec le mode de débogage activé lorsque le problème se produit (dans cet article, vous pouvez trouver comment collecter le fichier de diagnostic)

Informations connexes

- Guide de l'utilisateur Secure Endpoint
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.