Fehlerbehebung bei Exploit-Schutz in sicheren Endgeräten

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Geschützte Prozesse](#)
[Ausgeschlossene Prozesse](#)
[Exploit-Prävention Version 5 (Connector-Version 7.5.1 und höher)](#)
[Konfiguration](#)
[Erkennung](#)
[Fehlerbehebung](#)
[Erkennung von Fehlalarmen](#)
[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der Exploit Prevention Engine in der Secure Endpoint-Konsole und die Durchführung grundlegender Analysen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen.

- Administratorzugriff auf die Konsole für sichere Endgeräte
- Sicherer Endgeräteanschluss
- Exploit-Schutz aktiviert

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- Steckverbinder ab Version 7.3.15
- Windows 10 Version 1709 und höher oder Windows Server 2016 Version 1709 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das in diesem Dokument beschriebene Verfahren ist hilfreich, um eine grundlegende Analyse anhand der Ereignisse durchzuführen, die in der Konsole ausgelöst werden, und schlägt vor, Exploit Prevention-Ausschlüsse auszuschließen, falls Sie den Prozess kennen und ihn in Ihrer Umgebung verwenden.

Die Exploit-Prevention-Engine bietet die Möglichkeit, Ihre Endgeräte vor Angriffen durch Speicherinjektionen zu schützen, die üblicherweise von Malware und anderen Zero-Day-Angriffen auf nicht aktualisierte Software-Schwachstellen verwendet werden. Wenn ein Angriff auf einen geschützten Prozess erkannt wird, wird er blockiert und generiert ein Ereignis, das jedoch nicht in Quarantäne verschoben wird.

Geschützte Prozesse

Die Exploit-Prevention-Engine schützt diese 32-Bit- und 64-Bit-Prozesse (Secure Endpoint Windows Connector Version 6.2.1 und höher) sowie deren untergeordnete Prozesse:

- Microsoft Excel-Anwendung
- Microsoft Word-Anwendung
- Microsoft PowerPoint-Anwendung
- Microsoft Outlook-Anwendung
- Internet Explorer-Browser
- Mozilla Firefox-Browser
- Google Chrome-Browser
- Microsoft Skype-Anwendung
- TeamViewer-Anwendung
- VLC Media Player-Anwendung
- Microsoft Windows Script-Host
- Microsoft PowerShell-Anwendung
- Adobe Acrobat Reader
- Microsoft Register-Server
- Microsoft-Aufgabenplanungsmodul
- Microsoft-DLL-Befehl ausführen
- Microsoft HTML-Anwendungshost
- Windows Script-Host
- Microsoft Assembly Registration-Tool
- Zoom
- Schlank
- Cisco WebEx Teams
- Microsoft-Teams

Ausgeschlossene Prozesse

Diese Prozesse werden aufgrund von Kompatibilitätsproblemen von der Exploit-Präventions-Engine ausgeschlossen (nicht überwacht):

- McAfee DLP-Dienst
- McAfee Endpoint Security Utility

Exploit-Prävention Version 5 (Connector-Version 7.5.1 und höher)

Secure Endpoint Windows Connector 7.5.1 enthält ein wichtiges Update für die Exploit-Prävention. Zu den neuen Funktionen dieser Version gehören:

- Schutz von Netzlaufwerken: Schützt automatisch Prozesse, die von Netzlaufwerken aus ausgeführt werden, vor Bedrohungen wie Ransomware
- Schutz von Remote-Prozessen: Schützt automatisch Prozesse, die remote auf geschützten Computern ausgeführt werden, die einen domänenauthentifizierten Benutzer (Administrator) verwenden
- AppControl-Umgehung durch Rundll32: Stoppt speziell erstellte rundll32-Befehlszeilen, die interpretierte Befehle erlauben
- UAC-Umgehung: Blockiert die Rechteausweitung durch böswillige Prozesse und verhindert, dass die Windows-Benutzerkontensteuerung umgeht
- Browser-/Mimikatz-Tresoranmeldeinformationen: Wenn diese Option aktiviert ist, schützt Exploit Prevention in Microsoft Internet Explorer und den Edge-Browsern vor dem Diebstahl von Anmeldeinformationen.
- Löschen von Schattenkopien: Verfolgt das Löschen von Schattenkopien und fängt die COM-API im Microsoft Volume Shadow Copy Service (vssvc.exe) ab
- SAM-Hashes: Schützt vor dem Diebstahl von SAM-Hash-Anmeldeinformationen durch Mimikatz und fängt Versuche ab, alle SAM-Hashes in der Registrierungsstruktur aufzulisten und zu entschlüsseln
  Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users

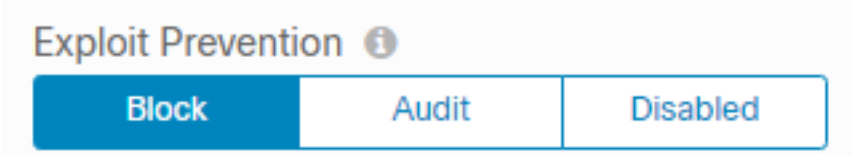
- Ausgeführte Prozesse schützen: Einschleusen in ausgeführte Prozesse, wenn diese vor der Exploit-Prevention-Instanz gestartet wurden (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Diese Funktionen sind standardmäßig aktiviert, wenn in der Richtlinie "Exploit-Prävention" aktiviert ist.

Konfiguration

Um die Exploit-Präventionsengine zu aktivieren, navigieren Sie zu **Modi und Engines** in Ihrer Policy und wählen Audit mode, Block mode oder Disabled mode, wie im Bild gezeigt.

> **Anmerkung:** Der Überwachungsmodus ist nur auf Secure Endpoint Windows Connector 7.3.1 und höher verfügbar. Frühere Versionen des Connectors behandeln den Überwachungsmodus wie den Blockmodus.

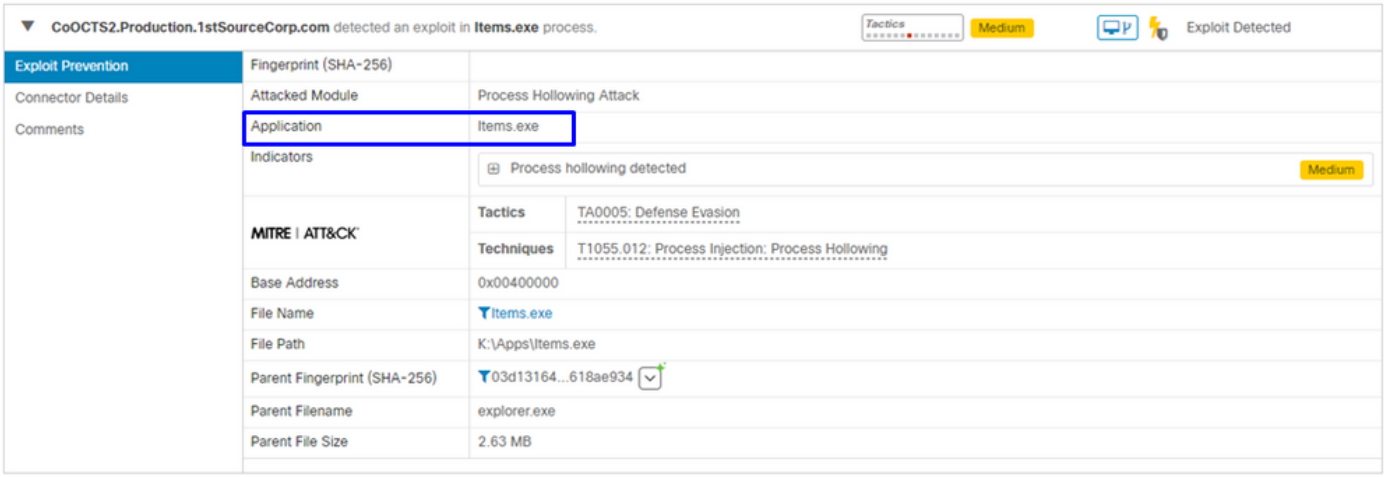


Anmerkung: Unter Windows 7 und Windows Server 2008 R2 müssen Sie den Patch für Microsoft Security Advisory 303929 anwenden, bevor Sie den Connector installieren.

Erkennung

Sobald die Erkennung ausgelöst wird, wird, wie im Bild dargestellt, eine Popup-Benachrichtigung auf dem Endpunkt angezeigt.

Die Konsole zeigt ein Exploit-Prevention-Ereignis an, wie im Bild dargestellt.

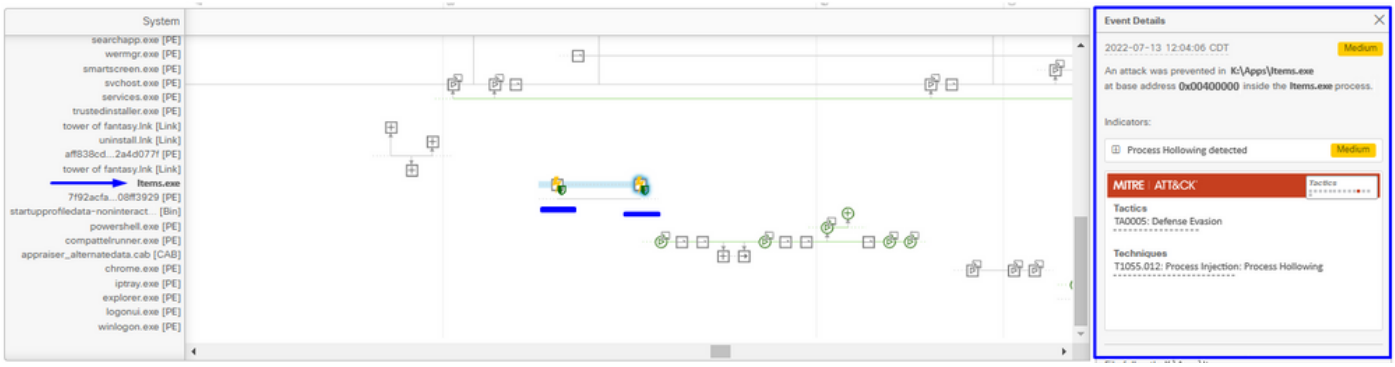


Fehlerbehebung

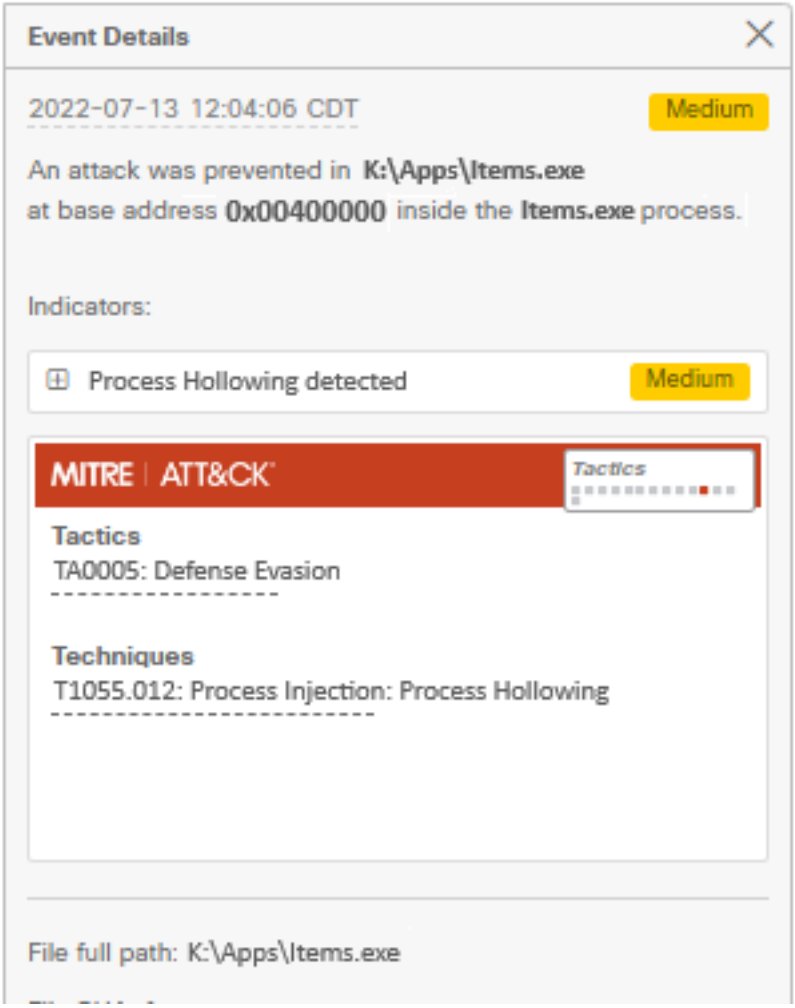
Wenn in der Konsole ein Exploit-Prevention-Ereignis ausgelöst wird, basiert die Identifizierung des erkannten Prozesses auf den Details. So erhalten Sie Einblick in die Ereignisse, die während der Ausführung der Anwendung oder des Prozesses aufgetreten sind, und können zur **Device Trajectory** navigieren.

Schritt 1: Klicken Sie auf das **Device Trajectory**-Symbol, das im Ereignis "Exploit-Verhinderung" angezeigt wird, wie im Bild gezeigt.

Schritt 2: Suchen Sie in der Zeitleiste der Device Trajectory nach dem Symbol "Exploit Prevention", um den Abschnitt **"Event Details" (Ereignisdetails)** anzuzeigen, wie im Bild dargestellt.



Schritt 3: Ermitteln Sie die Details des Ereignisses, und evaluieren Sie, ob der Prozess oder die Anwendung in Ihrer Umgebung vertrauenswürdig oder bekannt ist.



Erkennung von Fehlalarmen

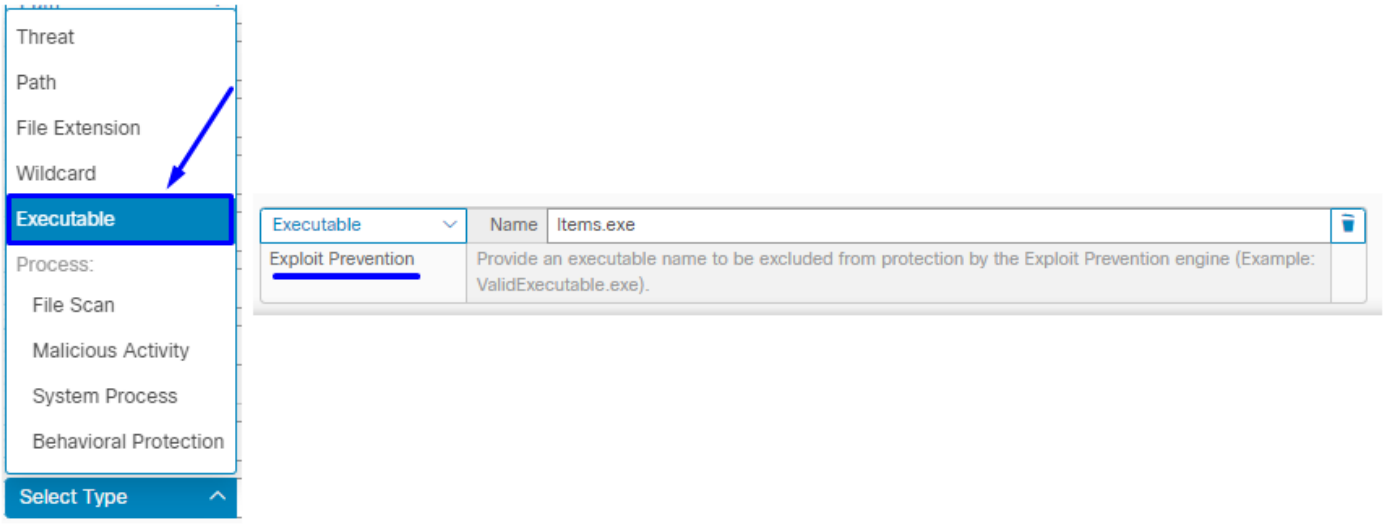
Sobald die Erkennung erkannt wurde und der Prozess bzw. die ausführbare Datei vertrauenswürdig und für Ihre Umgebung bekannt ist, kann sie als Ausschluss hinzugefügt werden. Um zu verhindern, dass der Steckverbinder scannt.

Ausgeschlossene ausführbare Dateien gelten nur für Connectors mit aktivierter Exploit-Prevention (Connector-Version 6.0.5 und höher). Ein Ausschluss ausführbarer Dateien wird verwendet, um bestimmte ausführbare Dateien von der Exploit-Präventionsengine auszuschließen.

> **Achtung**: Platzhalter und Erweiterungen außer exe werden nicht unterstützt.

Sie können die Liste der geschützten Prozesse überprüfen und beliebige Prozesse aus dem Exploit-Präventions-Modul ausschließen. Sie müssen den Namen der ausführbaren Datei im Feld für den Anwendungsausschluss angeben. Sie können auch alle Anwendungen von der Engine ausschließen. Ausschlüsse für ausführbare Dateien müssen genau mit dem Namen der ausführbaren Datei im Format **name.exe** übereinstimmen, wie im Bild gezeigt.

> **Anmerkung:** Alle ausführbaren Dateien, die Sie von der Exploit-Verhinderung ausschließen, müssen neu gestartet werden, nachdem der Ausschluss auf den Connector angewendet wurde. Wenn Sie die Exploit-Prävention deaktivieren, müssen Sie alle aktiven geschützten Prozesse neu starten.



> **Anmerkung:** Stellen Sie sicher, dass der Ausschlusssatz zur Richtlinie hinzugefügt wird, die auf den betroffenen Connector angewendet wird.

Schließlich können Sie das Verhalten überwachen.

Sollte die Erkennung von Exploit-Schutz weiterhin bestehen, wenden Sie sich an den TAC-Support, um eine tiefere Analyse durchzuführen. Hier finden Sie die erforderlichen Informationen:

- Screenshot des Ereignisses "Exploit-Prävention"
- Screenshot des Device Trajectory und Ereignisdetails
- SHA256 der betroffenen Anwendung/des betroffenen Prozesses
- Tritt das Problem bei deaktivierter Exploit-Prävention auf?
- Tritt das Problem bei deaktiviertem Secure Endpoint Connector-Dienst auf?
- Verfügt das Endgerät über andere Sicherheits- oder Antivirussoftware?
- Welche Anwendung ist betroffen? Funktion beschreiben
- Diagnosedatei (Debug-Paketprotokolle) mit aktiviertem Debugmodus, wenn das Problem auftritt (in diesem Artikel finden Sie Informationen zum Erfassen der Diagnosedatei)

Zugehörige Informationen

- Secure Endpoint - Benutzerhandbuch
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.