Risoluzione dei problemi di Exploit Prevention in Secure Endpoint

Sommario

Introduzione

In questo documento viene descritta la configurazione di Exploit Prevention Engine nella console Secure Endpoint e viene spiegato come eseguire un'analisi di base.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- Accesso amministrativo alla console dell'endpoint protetto
- Secure Endpoint Connector
- Funzionalità di prevenzione degli attacchi abilitata

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Connettore versione 7.3.15 o successiva
- Windows 10 versione 1709 e successive o Windows Server 2016 versione 1709 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

La procedura descritta in questo documento è utile per eseguire un'analisi di base basata sugli eventi, attivata nella console e suggerisce di sfruttare le esclusioni della prevenzione nel caso in cui si conosca il processo e lo si utilizzi nell'ambiente.

Il motore Exploit Prevention consente di difendere gli endpoint dagli attacchi tramite iniezione di memoria comunemente utilizzati dal malware e da altri attacchi a giorno zero su vulnerabilità software senza patch. Quando rileva un attacco contro un processo protetto, viene bloccato e generato un evento ma non viene messo in quarantena.

Processi protetti

Exploit Prevention Engine protegge questi processi a 32 bit e a 64 bit (Secure Endpoint Windows Connector versione 6.2.1 e successive) e i relativi processi figlio:

- Applicazione Microsoft Excel
- Applicazione Microsoft Word
- Applicazione Microsoft PowerPoint
- Applicazione Microsoft Outlook
- Browser Internet Explorer
- Browser Mozilla Firefox
- Google Chrome Browser
- Applicazione Microsoft Skype
- Applicazione TeamViewer
- Applicazione VLC Media Player
- Microsoft Windows Script Host
- Applicazione Microsoft Powershell
- Applicazione Adobe Acrobat Reader
- Registra server Microsoft
- Modulo di gestione Utilità di pianificazione Microsoft
- Comando Esegui DLL Microsoft
- Host applicazioni HTML Microsoft
- Windows Script Host
- Strumento di registrazione assembly Microsoft
- Zoom
- Margine di flessibilità
- Cisco Webex Teams
- Team Microsoft

Processi esclusi

Questi processi vengono esclusi (non monitorati) dal motore di prevenzione degli attacchi a causa di problemi di compatibilità:

- Servizio DLP McAfee

- Utilità McAfee Endpoint Security

Exploit Prevention versione 5 (Connector versione 7.5.1 e successive)

Secure Endpoint Windows Connector 7.5.1 include un aggiornamento significativo per la prevenzione degli attacchi. Le nuove funzionalità di questa versione includono:

- Protezione delle unità di rete: Protezione automatica dei processi eseguiti dalle unità di rete da minacce quali ransomware
- Protezione dei processi remoti: Protegge automaticamente i processi eseguiti in remoto in computer protetti che utilizzano un utente autenticato di dominio (admin)
- Bypass di AppControl attraverso rundll32: Arresta le righe di comando rundll32 create appositamente che consentono di eseguire i comandi interpretati
- Bypass controllo account utente: Blocca l'escalation dei privilegi da parte di processi dannosi, impedisce il bypass del meccanismo di controllo dell'account utente di Windows
- Credenziali insieme di credenziali browser/mimikatz: Se abilitata, la protezione da Exploit Prevention protegge contro il furto delle credenziali nei browser Microsoft Internet Explorer e Edge
- Eliminazione copia shadow: Tiene traccia dell'eliminazione delle copie shadow e intercetta l'API COM nel servizio Copia Shadow del volume di Microsoft (vssvc.exe)
- Hash SAM: Protegge contro il furto di credenziali hash SAM da parte di Mimikatz, intercetta i tentativi di enumerare e decrittografare tutti gli hash SAM nell'hive del Registro di sistema **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**

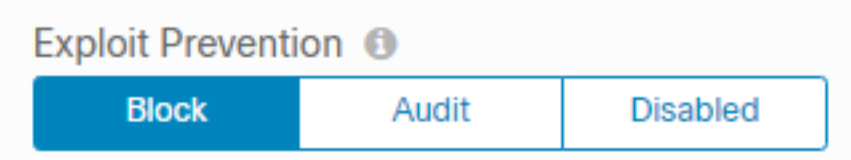
- Processi di protezione eseguiti: Eseguire l'inserimento nei processi che sono stati avviati prima dell'istanza di Exploit Prevention (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Queste funzionalità sono tutte abilitate per impostazione predefinita quando nei criteri è abilitata la protezione da attacchi.

Configurazione

Per abilitare il motore di prevenzione degli attacchi, passare a **Modalità e motori** nel criterio e selezionare Modalità di controllo, Modalità blocco o Modalità disabilitata, come mostrato nell'immagine.

> **Nota:** La modalità di controllo è disponibile solo sul connettore Secure Endpoint Windows 7.3.1 e versioni successive. Nelle versioni precedenti di Connector, la modalità di controllo è identica alla modalità blocco.

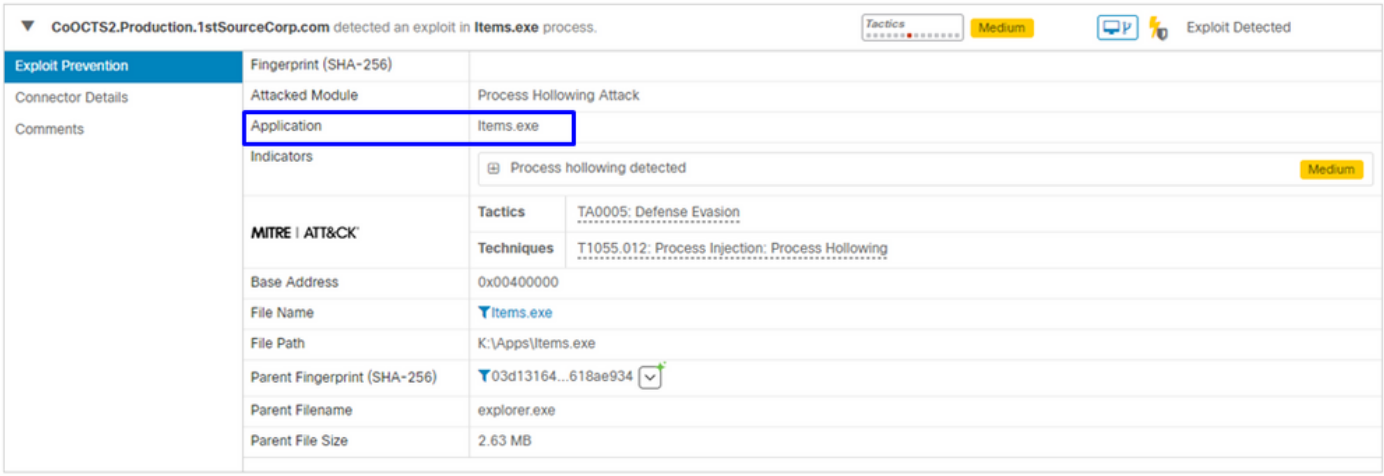


> **Nota:** In Windows 7 e Windows Server 2008 R2 è necessario applicare la patch per Microsoft Security Advisory 3033929 prima di installare il connettore.

Rilevamento

Una volta attivato il rilevamento, sull'endpoint viene visualizzata una notifica popup, come mostrato nell'immagine.

La console visualizza un evento di prevenzione dell'esplosione, come mostrato nell'immagine.

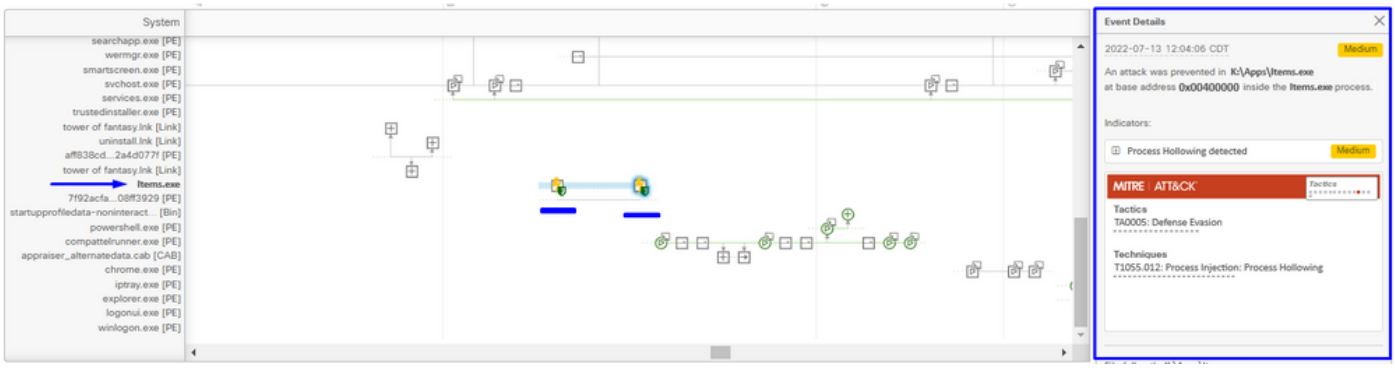


Risoluzione dei problemi

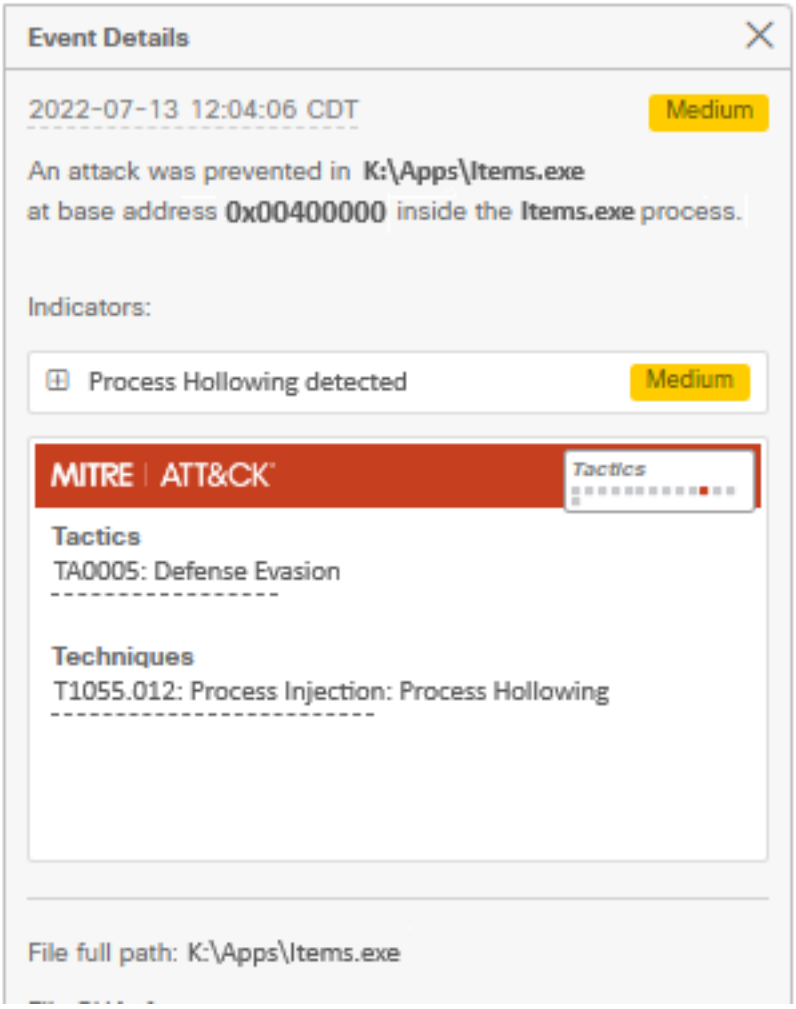
Quando nella console viene attivato un evento di prevenzione dell'esplosione, un modo per identificare il processo rilevato si basa sui dettagli per fornire visibilità sugli eventi che si sono verificati durante l'esecuzione dell'applicazione o del processo, è possibile passare alla **traiettoria** del **dispositivo**.

Passaggio 1. Fare clic sull'icona **Traiettoria periferica** visualizzata nell'evento di prevenzione dell'esplosione, come mostrato nell'immagine.

Passaggio 2. Individuare l'icona Exploit Prevention nella linea temporale della traiettoria del dispositivo per visualizzare la sezione **Event Details**, come mostrato nell'immagine.



Passaggio 3. Identificare i dettagli dell'evento e valutare se il processo o l'applicazione è attendibile/noto nell'ambiente.



Rilevamento falsi positivi

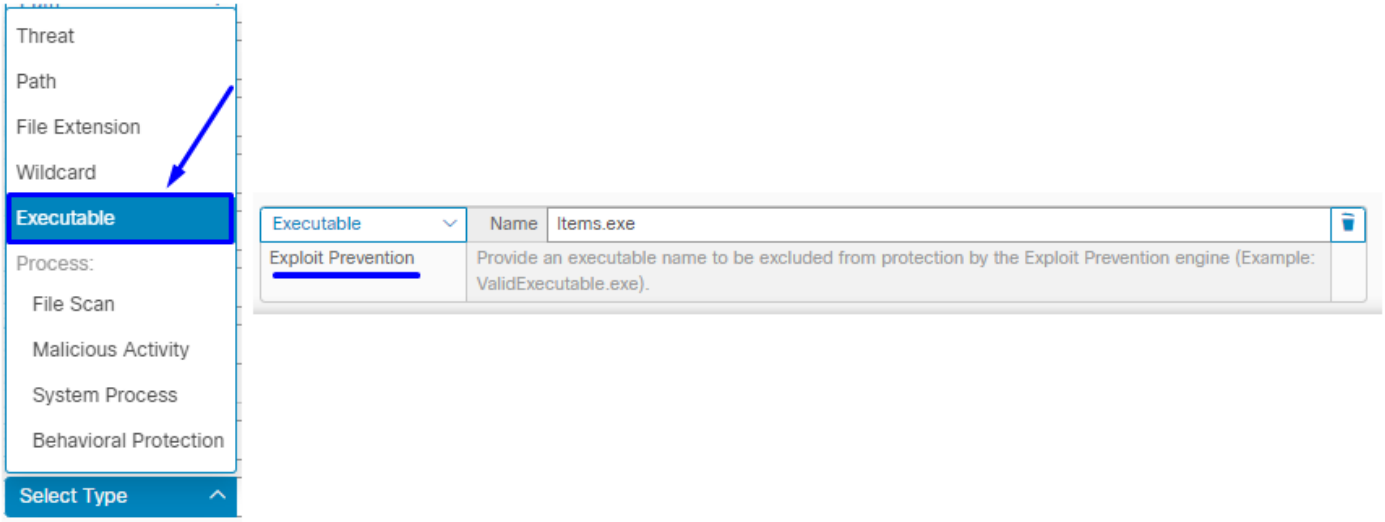
Una volta identificato il rilevamento e se il processo/eseguibile è attendibile e conosciuto dall'ambiente, è possibile aggiungerlo come esclusione. Per evitare che il connettore lo analizzi.

Le esclusioni dei file eseguibili si applicano solo ai connettori con la funzione di prevenzione dell'esplosione (Connector versione 6.0.5 e successive) abilitata. L'esclusione degli eseguibili viene utilizzata per escludere alcuni eseguibili dal motore di prevenzione dell'esplosione.

> **Attenzione**: i caratteri jolly e le estensioni diverse da exe non sono supportati.

Èpossibile controllare l'elenco dei processi protetti ed escluderne alcuni dal motore di prevenzione degli attacchi. È necessario specificare il nome del relativo eseguibile nel campo Esclusione applicazione. È inoltre possibile escludere qualsiasi applicazione dal motore. Le esclusioni degli eseguibili devono corrispondere esattamente al nome dell'eseguibile nel formato **name.exe**, come mostrato nell'immagine.

> **Nota:** Tutti gli eseguibili esclusi da Exploit Prevention devono essere riavviati dopo l'applicazione dell'esclusione al connettore. E se si disabilita la prevenzione dell'utilizzo, è necessario riavviare i processi protetti che erano attivi.



> **Nota:** Verificare che il set di esclusione sia aggiunto al criterio applicato al connettore interessato.

Infine, è possibile monitorare il comportamento.

Nel caso in cui il rilevamento Exploit Prevention persista, contattare il supporto TAC per eseguire un'analisi più approfondita. Qui è possibile trovare le informazioni necessarie:

- Schermata dell'evento Exploit Prevention
- Schermata della traiettoria del dispositivo e dei dettagli dell'evento
- SHA256 dell'applicazione/processo interessato
- Il problema si verifica quando la funzione di prevenzione degli attacchi è disabilitata?
- Il problema si verifica quando il servizio Connettore endpoint sicuro è disabilitato?
- L'endpoint dispone di altri software di protezione o antivirus?
- Qual è l'applicazione interessata? Descrizione della funzione
- File di diagnostica (registri del bundle di debug) con la modalità di debug attivata quando si verifica il problema (in questo articolo è possibile trovare come raccogliere il file di diagnostica)

Informazioni correlate

- Guida per l'utente di Secure Endpoint
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).