أستكشاف أخطاء مع الاستغلال وإصلاحها في نقطة نهاية آمنة

المحتويات

المقدمة

يصف هذا المستند تكوين محرك منع الاستغلال في وحدة تحكم نقطة النهاية الآمنة وكيفية إجراء التحليل الأساسي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية.

- وصول المسؤول إلى وحدة تحكم نقطة النهاية الآمنة
- Secure Endpoint Connector
- تمكين ميزة منع الاستغلال

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- الموصل الإصدار 7.3.15 أو إصدار أحدث
- Windows 10 الإصدار 1709 والإصدارات الأحدث أو Windows Server 2016 الإصدار 1709 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يعد الإجراء الموضح في هذا المستند مفيدا حول كيفية إجراء تحليل أساسي استنادا إلى الأحداث التي تم تشغيلها في وحدة التحكم ويقترح إستغلال إستثناءات "المنع" في حال كنت تعرف العملية وتستخدمها في بيئتك.

يوفر محرك Exploit Prevention (محرك منع الاستغلال) القدرة على الدفاع عن نقاط النهاية ديك من هجمات حقن الذاكرة التي تستخدم بشكل شائع من قبل البرامج الضارة والهجمات الأخرى التي لا تستغرق سوى يوم واحد على نقاط ضعف البرامج التي لم يتم تصحيحها. عندما يكتشف هجوم ضد عملية محمية فإنه يتم منعه ويولد حدثا لكنه ليس محجوبا.

عمليات محمية

يقوم محرك منع الاستغلال بحماية عمليات 32 بت و 64 بت هذه (الإصدار 6.2.1 من وما فوقها) والعمليات التابعة لها: Windows لنقطة النهاية الآمنة

- تطبيق Microsoft Excel
- تطبيق Microsoft Word
- تطبيق Microsoft PowerPoint
- تطبيق Microsoft Outlook
- متصفح Internet Explorer
- متصفح موزيلا فايرفوكس
- متصفح جوجل كروم
- تطبيق Microsoft Skype
- تطبيق TeamViewer
- تطبيق VLC Media Player
- مضيف البرنامج النصي لـ Microsoft Windows
- تطبيق Microsoft PowerShell
- تطبيق Adobe Acrobat Reader
- خادم التسجيل لـ Microsoft
- محرك جدولة المهام لـ Microsoft
- أمر Microsoft Run DLL
- مضيف تطبيق Microsoft HTML
- مضيف البرنامج النصي لـ Windows
- أداة تسجيل تجميع Microsoft
- تكبير
- نتوانى
- Cisco Webex Teams
- Microsoft Teams

العمليات المستبعدة

استبعدت هذه العمليات (ليس monitore) من Exploit Prevention محرك بسبب مشاكل التوافق:

- خدمة McAfee DLP
- أداة McAfee Endpoint Security Utility

Exploit Prevention الإصدار 5 (الموصل الإصدار 7.5.1 والإصدارات الأحدث)

يتضمن موصل Windows الآمن لنقطة النهاية 7.5.1 تحديثا هاما لمنع الاستغلال. تتضمن المميزات الجديدة في هذا الإصدار:

- حماية محركات الأقراص المتصلة بالشبكة: يوفر حماية تلقائية للعمليات التي يتم تشغيلها من محركات أقراص الشبكة ضد التهديدات مثل البرامج الخبيثة
- حماية العمليات عن بعد: يوفر حماية تلقائية للعمليات التي تعمل عن بعد على أجهزة كمبيوتر محمية تستخدم مستخدما مصدقا من المجال (مسؤول)
- تجاوز AppControl عبر Rundll32: توقف خطوط الأوامر Rundll32 المصممة خصيصا للسماح بتشغيل الأوامر التي تم تفسيرها
- تجاوز UAC: منع تصعيد الامتيازات بواسطة العمليات الضارة، يمنع آلية التحكم في حساب المستخدم ل Windows من تجاوز
- يخزن المستعرض/Mimikatz بيانات الاعتماد: إذا تم تمكينها، تعمل ميزة Exploit Prevention (منع الاستغلال) على توفير الحماية ضد سرقة بيانات الاعتماد في مستعرضي Microsoft Internet Explorer و Edge
- حذف نسخة الظل الاحتياطية: يتتبع حذف نسخ الظل الاحتياطية، ويعترض واجهة برمجة تطبيقات COM في Microsoft Volume Shadow Copy Service (vssvc.exe)
- تجزئة SAM: يوفر الحماية ضد سرقة بيانات اعتماد تجزئة SAM بواسطة Mimikatz، ويعترض محاولات تعداد عمليات تجزئة SAM في خلية السجل **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users** وفك تشفيرها

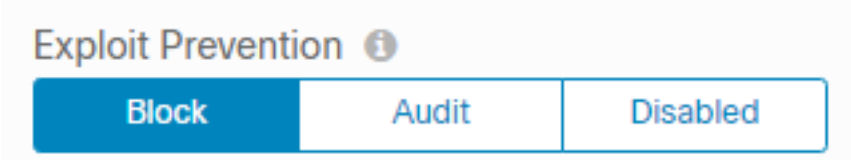
- عمليات الحماية التي تم تنفيذها: أدخل في عمليات قيد التشغيل، إذا كانت قد بدأت قبل مثيل Exploit Prevention (Explorer.exe و lsass.exe و spoolsv.exe و winlogon.exe)

يتم تمكين جميع هذه المميزات بشكل افتراضي عند تمكين "منع الاستغلال" في النهج.

التكوين

لتمكين محرك منع الاستغلال، انتقل إلى **الأوضاع والمحركات** في النهج وحدد وضع التدقيق أو وضع الحظر أو وضع التعطيل، كما هو موضح في الصورة.

> **ملاحظة**: لا يتوفر وضع التدقيق إلا على موصل Windows لنقطة النهاية الآمنة 7.3.1 والإصدارات الأحدث. تعامل الإصدارات السابقة من الموصل وضع التدقيق بنفس وضع الحظر.



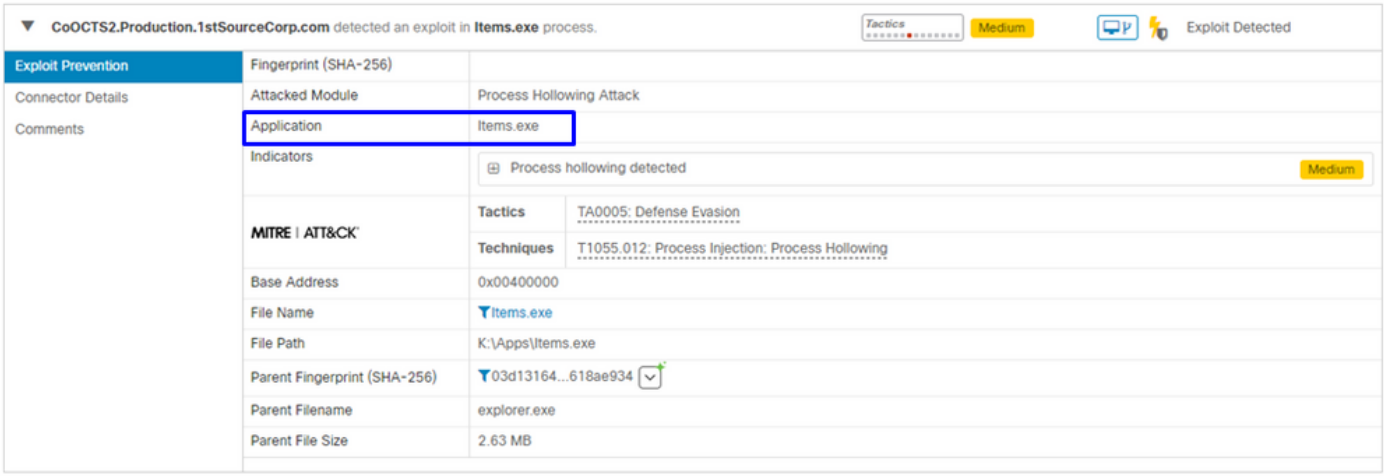
> **ملاحظة**: على نظام التشغيل Windows 7 و Windows Server 2008 R2، يجب تطبيق التصحيح على Microsoft Security Advisor 3033929 قبل تثبيت الموصل.

الكشف

بمجرد تشغيل الكشف، يتم عرض إعلام منبثق على نقطة النهاية، كما هو موضح في

الصورة.

تعرض وحدة التحكم حدث "منع الاستغلال"، كما هو موضح في الصورة.

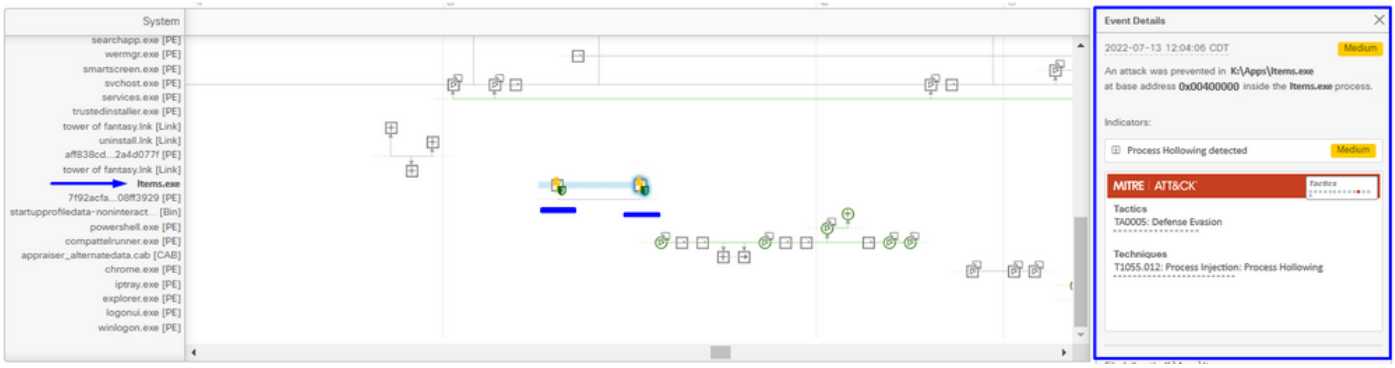


استكشاف الأخطاء وإصلاحها

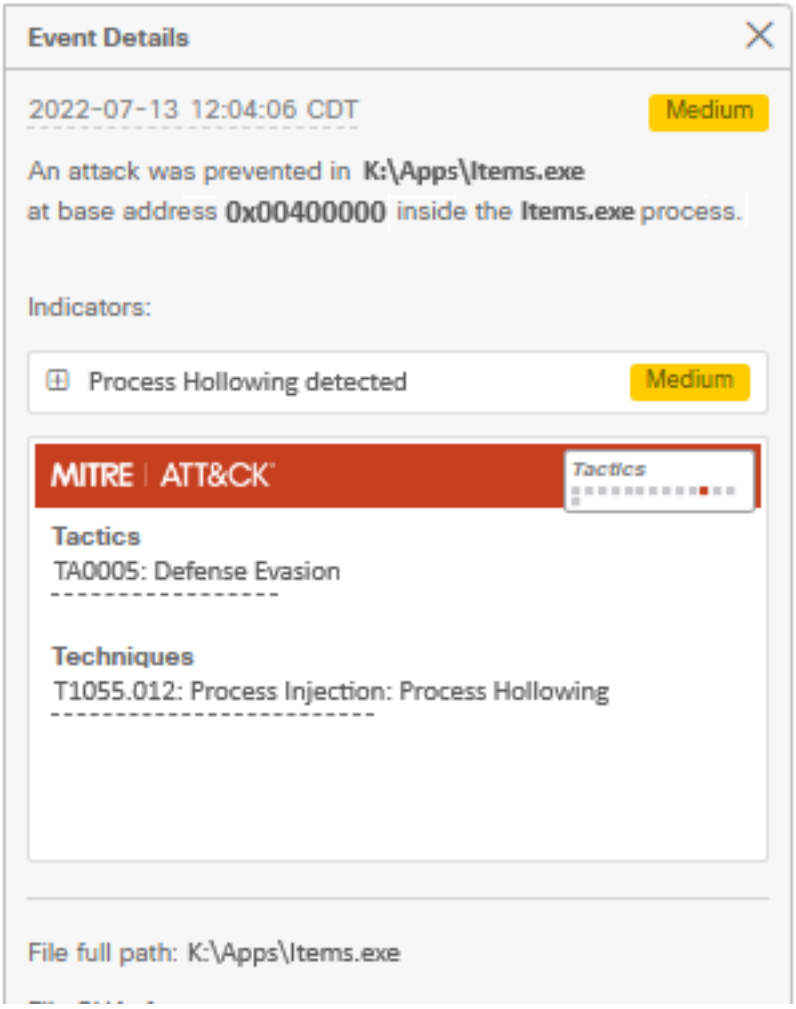
عند تشغيل حدث Exploit Prevention (منع الاستغلال) في وحدة التحكم، تعتمد طريقة لتحديد العملية التي تم الكشف عنها على التفاصيل لتوفير إمكانية الرؤية للأحداث التي حدثت أثناء تشغيل التطبيق أو العملية، يمكنك الانتقال إلى **مسار الهجاز**.

الخطوة 1. انقر على أيقونة **مسار الهجاز** التي تظهر في حدث منع الاستغلال، كما هو موضح في الصورة.

الخطوة 2. ابحث عن أيقونة منع الاستغلال في الخط الزمني لمسار الهجاز لترى قسم **تفاصيل الحدث**، كما هو موضح في الصورة.



الخطوة 3. حدد تفاصيل الحدث، وقم بتقييم ما إذا كانت العملية أو التطبيق موثوق به/معروف في بيئتك.



الكشف الإيجابي الكاذب

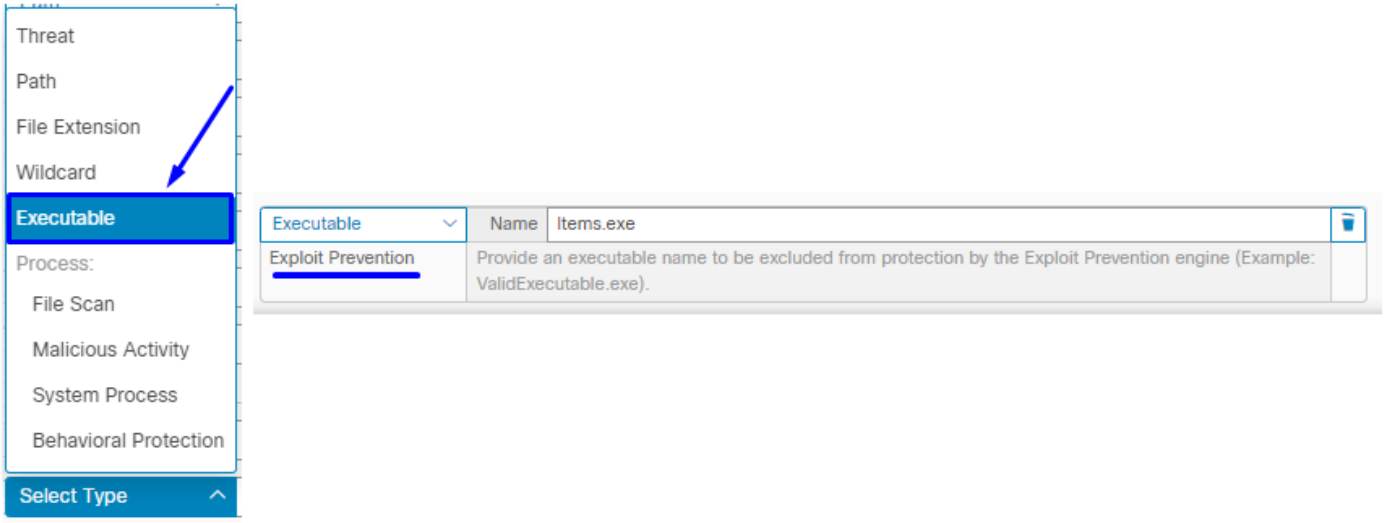
بمجرد تعريف الكشف وإذا كانت البيئة الخاصة بك تثق بالعملية/التنفيذ وتعرف عليهما، يمكنك إضافته كاستثناء. لمنع الموصل من إجراء الفحص عليه.

تنطبق الاستثناءات القابلة للتنفيذ فقط على الموصلات التي تم تمكين ميزة Exploit Prevention (الإصدار 6.0.5 من الموصل والإصدارات الأحدث). يتم إستخدام إستثناء قابل للتنفيذ لاستبعاد بعض الملفات التنفيذية من محرك منع الاستغلال.

> **تحذير**: لا يتم دعم أحرف البدل والامتدادات بخلاف exe.

يمكنك التحقق من قائمة العمليات المحمية واستبعاد أي من محرك منع الاستغلال، تحتاج إلى تحديد اسم التنفيذي في حقل إستثناء التطبيق. يمكنك أيضا إستبعاد أي تطبيقات من المحرك. تحتاج الاستثناءات القابلة للتنفيذ لمطابقة الاسم التنفيذي تماما في التنسيق **name.exe**، كما هو موضح في الصورة.

> **ملاحظة**: يجب إعادة تشغيل أي ملفات تنفيذية تستبعدها من "منع الاستغلال" بعد تطبيق الاستبعاد على الموصل. وإذا قمت بتعطيل "منع الاستغلال"، يجب إعادة تشغيل أي من العمليات المحمية التي كانت نشطة.



ملاحظة: تأكد من إضافة مجموعة الاستبعاد إلى السياسة المطبقة على الموصل المتأثر.

أخيرا، يمكنك مراقبة السلوك.

في حالة إستمرار اكتشاف Exploit Prevention (منع الاستغلال)، يرجى الاتصال بدعم TAC لإجراء تحليل أعمق. هنا يمكنك العثور على المعلومات المطلوبة:

- لقطة شاشة من حدث منع الاستغلال
- لقطة شاشة لمسار الجهاز وتفاصيل الحدث
- SHA256 للتطبيق/العملية المتأثرة
- هل تحدث المشكلة مع تعطيل منع الاستغلال؟
- هل تحدث المشكلة مع تعطيل خدمة موصل نقطة النهاية الآمنة؟
- هل تحتوي نقطة النهاية على أي برنامج أمان أو برنامج مكافحة فيروسات آخر؟
- ما هو التطبيق المتأثر؟ وصف الدالة
- ملف تشخيص (مجموعة تصحيح الأخطاء) مع تمكين وضع تصحيح الأخطاء عند حدوث المشكلة (في هذه الحالة يمكنك العثور على كيفية تجميع ملف التشخيص)

معلومات ذات صلة

- دليل مستخدم نقطة النهاية الآمنة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).