تكوين سلوك إغلاق أعطال DLP الذي يمنع إجراءات المستخدم أثناء فقدان الاتصال السحابي

المحتويات

مسألة

يواجه مستخدم تم تثبيت وحدة Endpoint DLP (EDLP) حظرا من الطباعة والنسخ إلى مشاركات ملفات الشبكة، بالرغم من عدم تضمينه في أي قواعد EDLP تم تكوينها. تم تكوين جميع قواعد EDLP الموجودة في وضع المراقبة مع تضمين 3 مستخدمين محددين فقط في هذه القواعد. كان المستخدم المتضرر يواجه إجراءات حظر غير متوقعة لعمليات الطباعة وعمليات نسخ مشاركة الملفات على الرغم من أنه لم يكن من المفترض أن تكون خاضعة لإنفاذ EDLP.

أثناء أستكشاف الأخطاء وإصلاحها، تم تحديد حدوث الحظر عندما كان اتصال سحابة EDLP غير متوفر، مما تسبب في قيام النظام بتطبيق السلوك المغلق عند الفشل آلية إحتياطية. تعرض المستخدم لرفض الطباعة والوصول إلى مشاركة الشبكة أثناء الفترات التي لم يقم فيها عميل EDLP بإنشاء اتصال بخدمة السحابة لإصدار أحكام النهج.

البيئة

- وحدة DLP لنقطة النهاية من Cisco، الإصدار 1.5.0.292
- إدارة بوابة منع الوصول الآمن/الأمان/فقد البيانات من Cisco
- تم تكوين قواعد EDLP متعددة في وضع المراقبة
- قناة مشاركة الشبكة التي تم تكوينها بسلوك إغلاق الفشل
- تغييرات دقة DNS التي تؤثر على اتصال شبكة العميل

رارق

تضمن الحل فهم وتفسير سلوك إغلاق أعطال EDLP وتطبيقه أثناء فقدان الاتصال السحابي:

تحليل السبب الجذري

كشف تحليل حزمة DART وسجلات EDLP عن تطبيق EDLP لرفض إحتياطي لأنه تم تكوين قناة مشاركة الشبكة كقناة مغلقة. في وقت حوادث الحظر، كان اتصال سحابة EDLP غير متوفر بسبب تغييرات تحليل DNS على شبكة العميل، مما منع النظام من الحصول على أحكام سياسة من خدمة السحابة.

شرح السلوك المغلق

تم تطبيق نهج الفشل المغلق على نظام المستخدم نظرا لتثبيت وحدة EDLP النمطية، بغض النظر عما إذا كانت هوية المستخدم مضمنة في أي قاعدة EDLP محددة. تعد حالة فتح/فشل-إغلاق إعداد عمومي موزود في تكوين نهج DLP، ويتم تطبيق تكوين القناة استنادا إلى هذا الإعداد العمومي.

إسترداد الاتصال

تم حل المشكلة تلقائيا بمجرد إستعادة إستقرار DNS على شبكة العميل، مما يسمح لعميل EDLP بإعادة إنشاء الاتصال بخدمة السحابة. لم يكن مطلوبا أي تدخل يدوي بمجرد حل مشكلة اتصال الشبكة الأساسية.

الظروف التي تؤدي إلى سلوك مماثل

يمكن أن تؤدي هذه الشروط إلى سلوك فشل EDLP المغلق:

- مشاكل تحليل DNS

- حالات انقطاع الشبكة
- التبديل بين الشبكات
- أي شرط يمنع الاتصال الشامل بين العميل وخدمة السحابة

السبب

حدث سلوك الحظر بسبب تكوين EDLP المغلق للفشل الخاص بقناة مشاركة الشبكة. عندما فقد عميل EDLP الاتصال بخدمة السحابة بسبب تغييرات تحليل DNS، لا يمكنه الحصول على أحكام النهج والتالي فرض السلوك الذي تم تكوينه إلغلاق الفشل كآلية إحتياطية للأمان. حدث هذا بغض النظر عما إذا كان قد تم تضمين المستخدم بشكل صريح في أي قواعد EDLP أم لا، نظرا لأن الإعداد الذي تم إغلاقه يطبق بشكل عام على جميع الأنظمة التي تم تثبيت وحدة EDLP النمطية فيها عندما يكون اتصال السحابة غير متوفر.

المحتوى ذي الصلة

- [الدعم الفني والتنزيلات من Cisco]

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).