AMP para console de endpoints e o último filtro visto

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Problema](#)
[Causa](#)
[Explicação de computadores "vistos recentemente" em um filtro de mais de 7 dias](#)
[Exemplo do mundo real](#)
[Solução de curto prazo](#)
[Solução de longo prazo](#)

Introduction

Este documento descreve a explicação do bug de filtro "Último Visto" referenciado ao CSCvh31177 na AMP (Advanced Malware Protection, proteção avançada contra malware) para endpoints.

Contribuído por Caly Hess, engenheiro da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao painel do Cisco AMP para endpoints

Componentes Utilizados

As informações neste documento são baseadas no software:

- Cisco AMP para endpoints para endpoints console versão 5.4.20190917

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O filtro "Última exibição" da página de computadores no console exibe os conectores que foram vistos nas últimas 24 horas que aparecem na lista.

Causa

A extração atual dos dados "Últimos vistos" é um trabalho singular a cada 24 horas. Embora os dados refletidos na página Computadores e a saída para Exportar para CSV para "Último Visto" sejam em tempo real, o próprio filtro executa os dados em lote desse trabalho singular. Isso foi implementado para aumentar a velocidade dos resultados, já

que a análise em tempo real dos timestamps para ambientes de grandes empresas pode levar a períodos de espera e bloqueio de banco de dados.

Explicação de computadores "vistos recentemente" em um filtro de mais de 7 dias

A máquina ficou off-line por mais de 7 dias até que o trabalho "Última exibição" foi executado.

Exemplo do mundo real

- HostA.randomdomain.net teve um acidente infeliz com uma caneca de café completa e a placa-mãe não recuperou completamente no dia 10 de agosto
- HostA.randomdomain.net está agora no depósito de reparos até 20 de setembro.
- Em 21 de setembro, o HostA.randomdomain.net retorna à rede 4 horas após a execução do trabalho "Último Visto", mas 2 horas antes do Auditor fazer uma Exportação para CSV dos computadores não vistos nos últimos 30 dias
- HostA.randomdomain.net ainda está listado do trabalho "Última exibição" como sendo mais de 30 dias não vistos. Apesar de agora estar totalmente funcional e sem café, o auditor agora o pega em sua exportação "inativa"

Solução de curto prazo

O trabalho em si não leva 24 horas completas para ser executado, mas pode levar pelo menos 12. Para aumentar a precisão do filtro, o reagendamento automático para o trabalho depois que o anterior for concluído está em desenvolvimento, o que deve ser cortado de 7 a 12 horas de folga na janela do lote.

Solução de longo prazo

Um retrabalho total do mecanismo "Último Visto" que está mais perto do tempo real quando os dados são puxados. Esta solução requer a implementação de uma estrutura de banco de dados totalmente nova que está atualmente em desenvolvimento com a versão proposta no próximo ano.