O filtro CSC-SSM URL falha com Corte-através da autenticação de proxy configurada na Em-linha ASA

Índice

Introdução

Este documento descreve o problema quando o filtro URL falha no módulo de Serviços de segurança satisfeito da Segurança e do controle (CSC-SSM) quando corte-através da autenticação de proxy é configurado na ferramenta de segurança adaptável (ASA) ou em um dispositivo entre a porta de gerenciamento do CSC-SSM e o Internet.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Circunstâncias/ambiente

O Authentication, Authorization, and Accounting (AAA) corte-através da autenticação de proxy é configurado em um ASA que esteja no trajeto entre a porta de gerenciamento do módulo CSC e o Internet.

Problema

Os Web site URL-não são filtrados com o CSC-SSM e o CSC-SSM HTTP. Os logs mostram as mensagens similares a estes:

```
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> Get URL Category returned [-1],
    with category 0 = [0] and rating = [0]
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> URLFilteringScanTask:PerformPreScanTask
    - URL rating failed, has to let it go
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> add result=1 server=
```

O problema é identificado facilmente depois que as capturas de pacote de informação são recolhidas a e da porta de gerenciamento do CSC-SSM na interface interna ASA. No exemplo abaixo, o endereço IP de Um ou Mais Servidores Cisco ICM NT da rede interna é 10.10.1.0/24 e o endereço IP de Um ou Mais Servidores Cisco ICM NT do módulo CSC é 10.10.1.70. O endereço IP 92.123.154.59 é o endereço IP de Um ou Mais Servidores Cisco ICM NT de um dos server da classificação de Trend Micro.

Quando o módulo CSC olha para determinar a categoria que uma determinada URL cai em, o módulo CSC deve pedir os server da classificação de Trend Micro para obter informações sobre dessa URL específica. As fontes CSC-SSM esta conexão de do seu próprio endereço IP de gerenciamento e ele usam o TCP/80 para uma comunicação. No display de tela acima, o aperto de mão da 3-maneira termina com sucesso entre o server da classificação de Trend Micro e o CSC-SSM. O CSC-SSM envia agora um pedido GET ao server e recebe uma” mensagem "HTTP/1.1 401 desautorizada gerada pelo ASA (ou pela outra em-linha dispositivo de rede) que faz corte-através do proxy.

Neste exemplo ASA, o AAA corte-através da autenticação de proxy é configurado com estes comandos:

```
aaa authentication match inside_authentication inside AUTH_SERV access-list
inside_authentication extended permit tcp any any
```

Estes comandos exigem o ASA alertar todos os usuários no interior (devido ao “tcp algum” na autenticação ACL) para que a autenticação vá a todo o Web site. O endereço IP de gerenciamento Do CSC-SSM é 10.10.1.70, que pertence à mesma sub-rede como aquele da rede interna é agora sujeito a esta política. Em consequência, o ASA considera o CSC-SSM ser apenas um outro host na rede interna e desafia-o para um nome de usuário e senha. Infelizmente, o CSC-SSM não está projetado fornecer a autenticação quando tenta alcançar os server da classificação de Trend Micro para a classificação das URL. Desde que o CSC-SSM falha a autenticação, o ASA envia uma” mensagem "HTTP/1.1 401 desautorizada ao módulo. A conexão fecha-se e a URL na pergunta não é classificada com sucesso pelo módulo CSC.

Solução

Use esta solução para resolver o problema.

Incorpore estes comandos isentar o endereço IP de gerenciamento do CSC-SSM da autenticação:

```
access-list inside_authentication extended deny tcp host 10.10.1.70 any access-list
inside_authentication extended permit tcp any any
```

A porta de gerenciamento Do CSC-SSM precisa de ter acesso completamente desimpedido ao Internet. Não deve atravessar nenhuma filtros ou verificações de segurança que puderam impedir o acesso ao Internet. Também, não deve ter que autenticar, em nenhuma maneira, de obter o acesso ao Internet.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems