Troubleshoot centralizou a quarentena PVO no ESA e no S A

Índice

[Introdução](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Compreenda a comunicação](#)
[Pesquise defeitos a entrega do ESA ao S A](#)
[Pesquise defeitos a entrega do S A ao ESA](#)
[TLS/Certificates](#)
[Informações Relacionadas](#)
[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento descreve como pesquisar defeitos a entrega e os problemas de conexão quando o quarnatine centralizado policiy, do vírus e da manifestação é permitido.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Envie por correio eletrónico a ferramenta de segurança (ESA) com AsyncOS 8.1 ou mais atrasado
- Dispositivo do Gerenciamento de segurança (S A) com AsyncOS 8.0 ou mais atrasado

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.

Informações de Apoio

Centralizado política, vírus e manifestação (PVO) quarentena característica era introduzido em AsyncOS 8.0) (ESA/8.1 (S A). Esta característica tem exigências adicionais da conectividade de rede, e levanta alguns desafios novos para pesquisar defeitos.

Compreenda a comunicação

- Uma comunicação CPQ usa o S TP, mas com alguns comandos extra para metadata de transferência

- O S A escutará as conexões na relação e na porta definidas sob serviços centralizados - > quarentena da política, do vírus e da manifestação. À revelia, a porta é 7025, mas esta pode ter sido mudada pelo usuário admin!
- O ESA escutará as conexões na relação e na porta definidas sob Serviços de segurança - > quarentena da política, do vírus e da manifestação. Além disso, à revelia, a porta é 7025, mas esta pode ter sido mudada pelo usuário admin!
- O S A igualmente usa o SSH (através do comando client) para obter a informação de configuração dos ESA. Em particular, isto é usado quando o S A entrega email liberados ao ESA. O S A usará o SSH para perguntar a configuração ESA e para determinar que /porta da relação para entregar o email liberado.

Ouvintes

- o ESA e o S A terão hidden um “cpq_listener chamado ouvinte” que escute na porta especificada.
- Estes ouvintes podem ser vistos no arquivo de configuração. Por exemplo:

```
<listener>
     <listener_name>cpq_listener</listener_name>
     <protocol>CPQ</protocol>
     <interface_name>Incoming Mail</interface_name>
     <port>7025</port>
     <listen_queue_size>50</listen_queue_size>
     <type>private</type>
     <hat>
$RELAYED
   RELAY {}
$BLOCKED
   REJECT {}
RELAYLIST:
   10.1.2.3
       $RELAYED (Only select hosts can relay from this box)
ALL
   $BLOCKED (Everyone else)
     </hat>
     <rat>
       <rat_entry>
         <rat_address>ALL</rat_address>
         <access>ACCEPT</access>
       </rat_entry>
     </rat>
```

- Estes ouvintes estarão suspendidos se o usuário admin usa “suspendlisteners todos” ou “suspenda”. Se a porta não está aceitando conexões, você deve verificar se o status de sistema é “autônomo” e resumo se necessário.

Pesquise defeitos a entrega do ESA ao S A

- Certifique-se do ESA possa conectar ao S A na porta configurada e na relação. Isto pode ser feito usando o telnet. Você deve obter uma bandeira 220 se a comunicação é bem sucedida.
- O ESA terá um objeto de destino chamado “the.cpq.host”, que contém mensagens quando for enfileirado para a entrega ao S A. Você pode ver este usar “tophosts” ou monitorá-lo - > estado da entrega. Você não pode usar o “hoststatus” com ele, mas você pode usar

"showrecipients" e "deleterecipients" caso necessário.

Pesquise defeitos a entrega do S A ao ESA

- Certifique-se do S A possa conectar ao ESA na porta configurada e na relação. Além disso, você pode usar o telnet e verá a bandeira 220 se bem sucedido.
- Ao usar conjuntos, é importante que a relação definida em Serviços de segurança inferiores nivelados do conjunto - > as quarentena da política, do vírus e da manifestação existem para todos os dispositivos a nível da máquina. (rede da verificação - > interfaces IP).
- O S A terá um objeto de destino chamado "the.cpq.release.host" que contém mensagens liberadas quando for enfileirado para a entrega ao ESA. Você pode ver este usar "tophosts". Isto não parece trabalhar com o "hoststatus" ou os "showrecipients", e eu não testei "deleterecipients" com ele, mas este provavelmente não trabalha qualquer um.
- Pode igualmente haver uns problemas com uma comunicação SSH entre o S A e o ESA. Estas edições não são sempre necessariamente baseados na rede, por exemplo em CSCus29647 um componente interno do S A sai da operação. As edições tais como estes aparecerão tipicamente como falhas do aplicativo nos logs do correio, e podem geralmente ser resolvidas recarregando o S A.

TLS/Certificates

- Todas as conexões CPQ em um ou outro sentido confiam no TLS, e em consequência a configuração da cifra pode jogar um papel.
- Para que a conexão TLS suceda, o dispositivo que abre a conexão deve poder verificar que o dispositivo receptor está usando nosso certificado hiddent CPQ. É possível para este falhar se o dispositivo negocia uma cifra anônima. Isto apareceria nos logs como qualquer outra coisa semelhante:

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- Você pode fixar estas edições simplesmente removendo as cifras anônimas da lista que parte da cifra da entrega, que é feita adicionando "`: - aNULL`" à extremidade da lista da cifra. Por exemplo: `ALTO: MEDIA:` **`- aNULL`**

Arquivo de registro

- Se o S A tem uma assinatura dos logs do correio (faz à revelia), você pode rever os logs do correio para recolher a introspecção adicional.
- CPQ que recebe eventos olhará como este para as mensagens que estão sendo quarantined ao S A e as mensagens liberadas ao ESA

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- Você pode procurar por estes eventos usando o grep, exemplo: `grep "mail_logs CPQ ICID"`
- Os eventos, ambos que quarantining do ESA e a liberação da entrega CPQ da quarentena do S A, olham similares a toda a outra entrega, com exceção a porta feita sob encomenda está listada e algumas linhas incluem a verbosidade "quarentena centralizada da política". Exemplo abaixo:

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
policy quarantine)
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

- Você pode encontrar estes eventos usando o grep ao seach para a porta, exemplo: `mail_logs porta 7025" do grep da "`

Botão do " habilitar " ESA desabilitado

Ao tentar permitir PVO no ESA, você pode encontrar que o botão do " habilitar " é esmaecida para fora, apesar de toda a configuração da condição prévia que está sendo terminada. Quando o ESA indica a página PVO, comunica-se com o S A sobre a porta 7025 para verificar que a configuração está pronta para ser permitido. Se esta comunicação falha, o botão do " habilitar " estará desabilitado. Você pode pesquisar defeitos este apenas como todo o ESA - > uma comunicação da porta 7025 S A grepping para a "porta 7025" no ESA. Para mais informação refira o TechNote alistado na informação relacionada.

Informações Relacionadas

- Exigências para o assistente da migração PVO quando o ESA for aglomerado
- A política de centralização ESA, o vírus, e a quarentena da manifestação (PVO) não podem ser permitidos