Pesquise defeitos falhas da atualização da alimentação da inteligência de Segurança no centro de gerenciamento de FireSIGHT

Índice

Introdução

Este documento descreve como pesquisar defeitos edições com atualizações da alimentação da inteligência de Segurança. A alimentação da inteligência de Segurança é compreendida de diversas lista regularmente actualizadas de endereços IP de Um ou Mais Servidores Cisco ICM NT que têm reputações deficientes, como determinado pela inteligência de Segurança de Cisco Talos e pelo grupo de investigação (Talos). É importante manter a alimentação da inteligência actualizada regularmente de modo que um sistema de Cisco FireSIGHT possa usar a informação atualizada a fim filtrar seu tráfego de rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Centro de gerenciamento de Cisco FireSIGHT
- Alimentação da inteligência de Segurança

Componentes Utilizados

A informação neste documento é baseada em um centro de gerenciamento de Cisco FireSIGHT que execute a versão de software 5.2 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.

Problema

Uma falha da atualização da alimentação da inteligência de Segurança ocorre. Você pode verificar a falha através da Web GUI ou do CLI (explicado mais nas seções que seguem).

Verifique o problema da Web GUI

Quando a falha da atualização da alimentação da inteligência de Segurança ocorre, o centro de gerenciamento de FireSIGHT indica alertas da saúde.

Verifique o problema do CLI

A fim determinar a causa de raiz de uma falha da atualização com a alimentação da inteligência de Segurança, incorpore este comando no CLI do centro de gerenciamento de FireSIGHT:

```
admin@Sourcefire3D:~$

cat /var/log/messages
```

Procure por qualquer um destes avisos nas mensagens:

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

Solução

Conclua estes passos para fazer o troubleshooting do problema:

1. Verifique que o local de *intelligence.sourcefire.com* é ativo. Navegue a https://intelligence.sourcefire.comin um navegador. Você deve receber uma cara do smiley, que indique que o local está vivo.

2. Alcance o CLI do centro de gerenciamento de FireSIGHT através do Shell Seguro (ssh).

3. Sibile *intelligence.sourcefire.com do* centro de gerenciamento de FireSIGHT:

   ```
   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.com
   ```

   Você deve receber uma saída similar a esta:

   ```
   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ms
   ```

   Se você não recebe uma resposta similar àquela mostrada, a seguir você pôde ter um

problema de conectividade de partida ou você não tem uma rota a *intelligence.sourcefire.com.*

4. Resolva o hostname para *intelligence.sourcefire.com*:

```
admin@Firepower:~$

sudo

nslookup intelligence.sourcefire.com
```

Você deve receber uma resposta similar a esta:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

Note: A saída acima mencionada usa o server do sistema do nome do public domain de Google (DNS) como um exemplo. A saída depende dos ajustes DNS que são configurados no **sistema > no Local > na configuração**, sob a seção da *rede*. Se você não recebe uma resposta similar àquela mostrada, a seguir assegure-se de que os ajustes DNS estejam corretos.**Caution**: O server usa um esquema do endereço IP de Um ou Mais Servidores Cisco ICM NT do arredondamento robin para o Balanceamento de carga, a tolerância de defeito, e o uptime. Consequentemente, os endereços IP de Um ou Mais Servidores Cisco ICM NT puderam mudar, e Cisco recomenda que o Firewall esteja configurado com um *CNAME* em vez de um endereço IP de Um ou Mais Servidores Cisco ICM NT.

5. Verifique a Conectividade a *intelligence.sourcefire.com* com o uso do telnet:

```
admin@Firepower:~$

 sudo telnet intelligence.sourcefire.com 443
```

Você deve receber uma saída similar a esta:

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

Note: Se você pode terminar com sucesso o segundo passo mas é incapaz ao telnet a *intelligence.sourcefire.com* sobre a porta 443, você pôde ter uma regra do Firewall que obstruísse a porta 443 de partida para *intelligence.sourcefire.com*.

6. Navegue ao **sistema > ao Local > à configuração** e verifique os ajustes do proxy da *configuração manual de proxy* sob a seção da *rede*.
Note: Se este proxy faz a inspeção do secure sockets layer (SSL), você deve pôr no lugar uma regra do desvio que contorneie o proxy para *intelligence.sourcefire.com*.
7. Teste se você pode executar um pedido *HTTP GET* contra *intelligence.sourcefire.com*:

```
admin@Firepower:~
```

```
sudo curl -vvk https://intelligence.sourcefire.com


* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<


:)


* Connection #0 to host intelligence.sourcefire.com left intact
```

Note: A cara do smiley na extremidade da saída do comando da *onda* indica uma conexão bem sucedida.**Note**: Se você usa um proxy, o comando da *onda* exige um username. O comando será **onda - <user> U - vvk** https://intelligence.sourcefire.com. Adicionalmente, depois que você incorpora o comando, você é alertado incorpora a senha do proxy.

8. Verifique que o tráfego HTTPS que é usado a fim transferir a alimentação da inteligência de Segurança não passa com um decryptor SSL. A fim verificar que nenhuma decriptografia de SSL ocorre, valide a informação do certificado de servidor na saída da etapa 6. Se o certificado de servidor não combina aquele indicado no exemplo que segue, a seguir você pôde ter um decryptor SSL que renunciasse o certificado. Se o tráfego passa com um decryptor SSL, você deve contornear todo o tráfego que vai a *intelligence.sourcefire.com*.

```
admin@Firepower:~$

sudo curl -vvk https://intelligence.sourcefire.com


* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA



* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl



*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
```

```
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<


:)


* Connection #0 to host intelligence.sourcefire.com left intact
```

Note: A decriptografia de SSL deve ser contorneada para a alimentação da inteligência de Segurança porque o decryptor SSL envia ao centro de gerenciamento de FireSIGHT um certificado desconhecido na saudação de SSL. O certificado que é enviado ao centro de gerenciamento de FireSIGHT não é assinado por CA Sourcefire-confiado, assim que pela conexão é não confiável.

Informações Relacionadas

- Falha automática da atualização da transferência em um centro de gerenciamento de FireSIGHT
- Endereços do servidor obrigatório para operações avançadas da proteção do malware (AMP)
- Portas de comunicação exigidas para a operação de sistema de FireSIGHT
- Suporte Técnico e Documentação - Cisco Systems