Como filtrar o código vermelho nos mecanismos de cache e conteúdo da Cisco

Índice

Introdução

Este documento fornece a informação em filtrar o worm de código vermelho no Cisco Cache e no Content Engine.

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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Configurações

Vários caches transparentes estão sendo sobrecarregados ao tentar conectar com sites inexistentes. Este documento fornece uma solução de filtragem do worm Código Vermelho que pode afetar as soluções de cache da Cisco. O worm Código Vermelho usa uma exploração de excesso de buffer em um script default.ida no IIS (Internet Information Servers). O código vermelho usa este pedido do Hypertext Transfer Protocol (HTTP):

```
get http://random-ip-address/default.ida?long-string-of-data
```

O long-string-of-data do exemplo acima é o excesso de buffer e código de instrução do worm propriamente dito. Você pode filtrar isto utilizando uma regra de bloco que use um URL-regex para corresponder o conteúdo. Para o hardware do Cisco Cache Engine que executam o software CE2.XX, e o hardware do Cisco Content Engine que executa o software 2.XX ou 3.XX, configurar como segue:

```
rule enable
rule block url-regex ^http://.*/default\.ida$
rule block url-regex ^http://.*www\.worm\.com/default\.ida$
```

Emita o **comando show rule all** indicar o número de pressionamentos que acumula contra esta regra de bloqueio. Para o hardware do Content Engine que executa o software 3.XX, você pode ser mais específico e não obstruir o pedido, mas a reescrita a um servidor de Web local indicar que seu local está contaminado. Use uma regra similar a esta:

```
rule enable
rule rewrite url-regsub ^http://.*/default\.ida$ http://local-webserver/codered.html
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Apoio de produtos de comunicação de rede de conteúdo
- Downloads do software Cisco Cache Engine 3.0 (somente clientes registrados)
- Downloads do software Cisco Cache Engine 2.0 (somente clientes registrados)
- Suporte Técnico - Cisco Systems