Usando assinaturas de série personalizada de verificação de repetição do Cisco Secure IDS/NetRanger para excesso de buffer remoto de worm “de código vermelho” na extensão ISAPI do indicador de servidor Microsoft em IIS 4.0 e 5.0

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Assinaturas de série personalizadas de verificação de repetição
Assinatura 1 — Acesso ao indicador do servidor com tentativa de exploração
Assinatura 2 — Worm do “código vermelho” do sobrefluxo de buffer de acesso ao servidor de indexação
Informações Relacionadas

Introdução

Até o final de julho de 2003, a Computer Economics (uma organização independente de pesquisa de Carlsbad, CA) estima que o worm Code Red tenha custado às empresas US$ 1,2 bilhão para recuperação dos danos na rede e em perda de produtividade. Esta avaliação aumentou significativamente com a versão subsequente do “do worm mais poderoso código vermelho II”. O Cisco Secure Intrusion Detection System (IDS), um componente-chave do Cisco SAFE Blueprint, tem se mostrado de grande utilidade na detecção e redução dos riscos de segurança de rede, incluindo o worm "Code Red" (Código Vermelho).

Este documento descreve uma atualização de software para detectar o método de exploração usado pelo worm "Código Vermelho" (consulte Assinatura 2, a seguir).

Você pode criar as assinaturas de fsérie personalizada de verificação de repetição mostradas abaixo para travar a exploração de um excesso de buffer para os servidores de Web que executam Microsoft Windows NT e Internet Information Services (IIS) 4.0 ou Windows 2000 e IIS 5.0. Observe também que o serviço de indexação no Windows XP Beta também é vulnerável. A Recomendação de Segurança que descreve esta vulnerabilidade está em http://www.eeye.com/html/Research/Advisories/AD20010618.html . Microsoft liberou uma correção de programa para esta vulnerabilidade que pode ser transferida de http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx .

As assinaturas discutidas neste documento tornaram-se disponíveis na liberação da atualização de assinatura S(5). O Cisco Systems recomenda que os sensores estejam promovidos a 2.2.1.8 ou à atualização de assinatura 2.5(1)S3 antes de executar esta assinatura. Os usuários registrados podem transferir estas atualizações de assinatura do centro do Software Seguro Cisco. Todos os usuários podem entrar em contato com o Suporte Técnico da Cisco por e-mail e telefone usando os contatos mundiais da Cisco.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de software:

- Microsoft Windows NT e IIS 4.0
- Microsoft Windows 2000 e IIS 5.0

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.

Assinaturas de série personalizadas de verificação de repetição

Há duas assinaturas de fsérie personalizada de verificação de repetição específicas para endereçar esta edição. Cada assinatura é descrita abaixo, e as configurações de produto aplicáveis são fornecidas.

Assinatura 1 — Acesso ao indicador do servidor com tentativa de exploração

Essa assinatura aciona uma tentativa de sobrefluxo de buffer na Extensão ISAPI do Serviço de Indexação combinada com uma tentativa de passar o código shell para o servidor a fim de obter acesso privilegiado na forma original do código. A assinatura é lançada apenas na tentativa de passar código shell para o serviço de destino ao se tentar obter acesso integral de nível de SISTEMA. Um possível problema é que a assinatura não será lançada se o atacante não tentar passar qualquer tipo de código shell e só executar o excesso de buffer contra o serviço em uma tentativa de travar o IIS e criar uma recusa de serviço.

Série

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Configurações do produto

- Ocorrências: 1
- Porta: 80

Nota: Se você tem vários servidores escutando em outras portas TCP (por exemplo, 8080), precisará criar uma correspondência de séries personalizadas separada para cada número de porta.

- Nível de severidade do alarme recomendado:Alto (Cisco Secure Policy Manager)5 (Unix Director)
- Direção:PARA

Assinatura 2 — Worm do “código vermelho” do sobrefluxo de buffer de acesso ao servidor de indexação

Os segundos fogos da assinatura em um excesso de buffer tentado na extensão isapi do servidor de indexação combinada com uma tentativa de passar o código do shell ao server para ganhar o acesso de privilegiado no formulário confundido que o worm do “código vermelho” usa. Esta assinatura ateia fogo somente na tentativa de passar o código do shell ao serviço de destino na tentativa de ganhar o acesso nivelado do sistema cheio. Um possível problema é que a assinatura não será lançada se o atacante não tentar passar qualquer tipo de código shell e só executar o excesso de buffer contra o serviço em uma tentativa de travar o IIS e criar uma recusa de serviço.

Série

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Nota: Não há nenhum espaço em branco na corda acima.

Configurações do produto

- Ocorrências: 1
- Porta: 80

Nota: Se você tem vários servidores escutando em outras portas TCP (por exemplo, 8080), precisará criar uma correspondência de séries personalizadas separada para cada número de porta.

- Nível de severidade do alarme recomendado:Alto (Cisco Secure Policy Manager)5 (Unix Director)
- Direção:PARA

Para obter mais informações sobre do Cisco Secure IDS, refira o Cisco Secure Intrusion Detection.

Informações Relacionadas

- Suporte técnico – Roteadores
- Consultivos de segurança Cisco
- Página de suporte do Cisco Secure Intrusion Detection

- Suporte Técnico - Cisco Systems