Procedimentos de emergência de recuperação de desastre do Código Vermelho II para uma rede AVVID

Índice

Introdução

Este documento aborda os procedimentos para eliminar imediatamente a maioria dos efeitos colaterais do Cisco CallManager causados por uma infecção de Código Vermelho II generalizada, assim como as soluções de curto e longo prazo para proteger melhor uma rede AVVID contra problemas futuros relacionados à essa infecção.

Pré-requisitos

Requisitos

Os leitores deste documento devem estar cientes destes tópicos:

- A administração do CallManager da Cisco
- Procedimento de emergência para recuperação de desastres

Componentes Utilizados

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

- Cisco CallManager 3.x
- Microsoft Windows 2000
- Todas as versões do Cisco Unity

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.

Ações imediatas

Conclua estes passos:

1. Execute a vitória-OS-elevação a mais atrasada (disponível na seção cripto da página apropriada da transferência da versão do CallManager no CCO) em todos os server da Telefonia IP que executam o Windows 2000, e execute o utilitário de reparo apropriado (Microsoft tem uma ferramenta disponível) e/ou manualmente (disponível da McAfee) feche as portas traseiras criadas pelo código vermelho II. Para servidores de telefonia IP executando o NT4.0 IIS, instale o Service Pack 6a e, em seguida, a correção Code Red.**Caution**: Como este worm cria acessos para invasões, se o servidor foi diretamente conectado à Internet e alguém colocou mais acessos para invasões nele, enquanto comprometido, ou se existir a possibilidade de o servidor ser futuramente comprometido de dentro de sua rede, a ação mais segura será fazer uma cópia de segurança dos dados e reinstalar o servidor do início.
2. Pare e desabilite o serviço IIS Admin e o Serviço de Publicação na Web em todos os assinantes do CallManager da Cisco, e o todo o server que não os exigir. Esses serviços devem permanecer ativos no Cisco CallManager Publisher.Para executar essa tarefa, siga estes passos:Traga acima aos serviços o applet indo ao **iniciar > programas > ferramentas administrativas > serviços**.Clique com o botão direito do mouse em IIS Admin Service (Serviço de Administração do IIS) e selecione Stop (Parar). Isto igualmente para o Serviço de Publicação na Web.Clicar com o botão direito o **serviço IIS Admin** e selecione **propriedades**. Altere o Startup Type para Disable e feche a janela.Clicar com o botão direito o **world wide web que publica** e selecione **propriedades**. Altere o Startup Type para Disable e feche a janela.
3. Corrija ou repare todos os servidores IIS conhecidos na rede.
4. A distribuição atualizou as cargas de telefone.Para sistemas do Cisco CallManager 3.0X, transferência ciscocm_3-0-11_spA.exe do cisco.com. Da página do ccmadmin vá aos **padrões do sistema > do dispositivo** e ajuste as cargas do dispositivo de 7940/7960 ao **P003E310**. Clique em **Update**.Para sistemas Cisco CallManager 3.1x, faça o download do arquivo ciscocm_3-1-1_spA.exe do site Cisco.com. Da página do ccmadmin vá aos **padrões do sistema > do dispositivo** e ajuste as cargas do dispositivo de 7940/7960 ao **P00303010100**. Clique em **Update**.Para ambo o 3.0 e 3.1 do CallManager da Cisco, vá ao **sistema > ao grupo do CallManager**. Selecione o primeiro grupo no lado esquerdo e clique em Reset Devices (Reinicializar Dispositivos). Quando solicitado, clique em OK. Faça isso para cada grupo do Cisco CallManager presente nos telefones para obter novos carregamentos.O Cisco CallManager 3.2x e os sistemas 3.3x não exigem uma carga actualizado do telefone, porque inclui todos os reparos necessários.
5. Identifique e tome de servidores IIS contaminados permanecendo na rede (isto poderia

facilmente esticar em uma solução de termo próximo, segundo quantos servidores IIS desonestos estão na rede). Aqui há dois métodos:No servidor de publicação do CallManager da Cisco, ou em todo o outro servidor IIS com o registro permitido, vá a **c:\winnt\system32\logfiles\w3svc1** e alcance o arquivo de registro o mais recente. Esses arquivos possuem uma convenção de nomeação do tipo ex000000.log.Procure uma linha semelhante a essa:

```
2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET /default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u6858%ucbd3%u7801%u9090%u9090%u8190%u 00c3%u0003%u8b00%u531b%
u53ff%u0078%u0000%u00=a200 -
```

Nesse caso, o endereço IP 172.20.148.189 está no servidor de ataque. Encontre o e a correção de programa ou limpe-a, ou desligue-a da rede.Repita este processo até que todos os servidores infectados pelo Código Vermelho sejam localizados e limpos.Um outro método é usar o utilitário livre disponível do eEye - CodeRedScanner. Esta utilidade faz a varredura de um C da classe de cada vez que procura as máquinas infectadas e as máquinas vulneráveis a um ataque baseado .ida. o eEye tem um varredor da classe B disponível para um custo adicional.

Soluções de curto prazo

- Verifique se o QoS está configurado corretamente na rede para priorizar o tráfego de voz em relação ao de dados. Para ajudar a assegurar-se de que a Qualidade de voz esteja afetada o menos possível durante o restante de operações de limpeza, refira as recomendações fornecidas nas soluções de rede de comunicação de Cisco e os guias do projeto QoS e os Guias de Design da solução de telefonia do IP Cisco.
- Estabelece VLANs separadas para voz e dados, seguindo os recursos do Cisco IP Telephony Solutions (Soluções de telefonia IP Cisco). Esta podia ser uma solução a longo prazo segundo o tamanho e a complexidade da rede envolvida.

Soluções de longo prazo

Uma vez que a emergência imediata se acaba, refira o COFRE FORTE: Segurança de telefonia IP detalhada. Este documento fornece informações sobre melhores práticas às partes interessadas, para o projeto e implementação de redes seguras de telefonia IP .

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems