Como o Cisco Secure IDS responde ao vírus Nimda

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
O Cisco IDS Host Sensor protege contra Nimda
O sensor de rede do Cisco IDS identifica NIMDA
Cursos de ação recomendados
Informações Relacionadas

Introdução

Este documento explica como o IDS (Sistema de Detecção de Intrusão) identifica e impede o comprometimento do servidor da web devido a ataques pelo vírus Nimda (também conhecido como vírus Concept). O complexo funcionamento técnico do worm está fora do escopo desse boletim e está bem documentado em outro local. Uma das melhores descrições técnica do worm de Nimda pode ser encontrado no worm de Nimda CA-2001-26 consultivo CERT® .

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

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

Informações de Apoio

O worm de Nimda é um worm e um vírus híbridos que esteja espalhando agressivelmente no Internet. Para compreender Nimda e as capacidades do Cisco IDS abrandar sua propagação, é importante definir estes dois termos:

- O worm refere-se a um código malicioso que se espalha automaticamente, sem intervenção humana.
- **O vírus** refere o código malicioso que espalha através de algum tipo de intervenção humana, como quando você abre um email, consulta uma site da web infectado, ou executa manualmente um arquivo infectado.

O worm de Nimda é realmente um híbrido que exiba características de um worm e de um vírus. O Nimda infecta de várias maneiras, a maioria delas exigem intervenção humana. Métodos de infecção similares a verme dos blocos de sensor do host do Cisco IDS que espalharam com as vulnerabilidades no Internet Information Server de Microsoft (IIS). O Cisco IDS não obstrui vírus-como, métodos de infecção manuais, como quando você abre um anexo de e-mail, consulta uma site da web infectado, ou execute manualmente um arquivo infectado.

O Cisco IDS Host Sensor protege contra Nimda

O sensor do host do Cisco IDS impede os ataques do passagem de diretório, que incluem aqueles usados pelo worm de Nimda. Quando o worm tenta comprometer um servidor de Web IDS-protegido Cisco, o ataque falha e o server não é comprometido.

Estas regras do sensor do host do Cisco IDS impedem o sucesso do worm de Nimda:

- Passagem de diretório IIS (quatro regras)
- Directory Traversal e execução de código de IIS (quatro regras)
- IIS Double Hex Encoding Directory Traversal (quatro regras)

O sensor do host do Cisco IDS igualmente defende contra alterações não autorizadas ao conteúdo da Web, assim que não permite que o worm altere página da web a fim espalhar-se a outros server.

O Cisco IDS está em conformidade com as melhores práticas de segurança padrão para proteger servidores de web contra o Nimda. Estes melhores prática ditam para não ler o email ou consultar a Web de um servidor de Web da produção, assim como para não ter partes da rede abra em um server. O sensor do host do Cisco IDS impede que o servidor de Web esteja comprometido com as façanhas HTTP e IIS. Os melhores prática acima mencionados asseguram-se de que o worm de Nimda não chegue no servidor de Web por alguns meios manuais.

O sensor de rede do Cisco IDS identifica NIMDA

O sensor de rede do Cisco IDS identifica os ataques de aplicativo da Web, que incluem aqueles usados pelo worm de Nimda. O sensor de rede pode identificar ataques e fornecer detalhes sobre o afetado ou os host comprometido para isolar a infecção nimda.

Fogo destes alarmes do sensor de rede do Cisco IDS:

- Acesso do WinNT cmd.exe WWW (SigID 5081)
- O dobro IIS CGI descodifica (SigID 5124)
- WWW IIS Unicode Attack (SigID 5114)

- IIS Dot Dot Execute Attack (SigID 3215)
- IIS Dot Dot Crash Attack (SigID 3216)

Os operadores não veem um alarme que identifique Nimda por nome. Veem uma série dos alarmes notáveis como façanhas diferentes das tentativas de Nimda para comprometer o alvo. Os alarmes identificam o endereço de origem dos anfitriões que foram comprometidos e que devem ser isolados da rede, ser limpados, e remendado.

Cursos de ação recomendados

Siga estas etapas para proteger contra o worm de Nimda:

1. Aplique as atualizações as mais atrasadas para o Microsoft outlook, o Outlook Express, o internet explorer, e o IIS disponível de Microsoft .
2. Atualize o software de exploração de vírus com a correção mais recente para atenuar a propagação do vírus.**Nota:** Você pode transferir a correção de vírus a mais atrasada para proteger seu PC da infecção. Se seu PC tem sido contaminado já, esta correção de vírus permite que você faça a varredura manualmente do disco rígido de seu PC e limpe a infecção da máquina.
3. Distribua o Cisco IDS para abrandar a ameaça, contenha a infecção, e proteja os server.

Informações Relacionadas

- Como proteger sua rede contra o vírus Nimda
- Consultivos e alertas de segurança de produto Cisco
- Página de suporte do Cisco Secure Intrusion Detection
- Suporte Técnico - Cisco Systems