Como o Cisco Secure IDS responde ao vírus Nimda

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Conventions
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

Introduction

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 técnicas do worm Nimda pode ser encontrada no verme de Nimda Nimda Advisory CA-2001-26 da CERT® .

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

O verme Nimda é um verme híbrido e um vírus que está se espalhando agressivamente na

Internet. Para entender o Nimda e as habilidades do Cisco IDS para atenuar sua propagação, é importante definir estes dois termos:

- **O worm refere-se a um código malicioso que se espalha automaticamente, sem intervenção humana.**
- **Vírus** refere-se a um código mal-intencionado que se espalha através de algum tipo de intervenção humana, como quando você abre um e-mail, navega em um site infectado ou executa manualmente um arquivo infectado.

O verme Nimda é, na verdade, um híbrido que exibe características tanto de um verme quanto de um vírus. O Nimda infecta de várias maneiras, a maioria delas exigem intervenção humana. O Cisco IDS Host Sensor bloqueia métodos de infecção semelhantes a worms que se espalham por vulnerabilidades no Internet Information Server (IIS) da Microsoft. O Cisco IDS não bloqueia métodos de infecção manuais semelhantes a vírus, como quando você abre um anexo de e-mail, navega em um site infectado ou executa manualmente um arquivo infectado.

O Cisco IDS Host Sensor protege contra Nimda

O Cisco IDS Host Sensor evita ataques de Diretório Transversal, incluindo os usados pelo worm Nimda. Quando o worm tenta comprometer um servidor Web protegido pelo Cisco IDS, o ataque falha e o servidor não é comprometido.

Essas regras do Cisco IDS Host Sensor impedem o sucesso do worm Nimda:

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

O Cisco IDS Host Sensor também defende contra alterações não autorizadas no conteúdo da Web, portanto, ele não permite que o worm altere as páginas da Web para se espalhar para outros servidores.

O Cisco IDS está em conformidade com as melhores práticas de segurança padrão para proteger servidores de web contra o Nimda. Essas práticas recomendadas exigem que não se leia e-mails ou navegue na Web a partir de um servidor Web de produção, bem como que não haja compartilhamentos de rede abertos em um servidor. O Cisco IDS Host Sensor impede que o servidor Web seja comprometido por meio de explorações HTTP e IIS. As práticas recomendadas acima garantem que o worm Nimda não chegue ao servidor Web por algum meio manual.

O sensor de rede do Cisco IDS identifica NIMDA

O Cisco IDS Network Sensor identifica ataques de aplicativos da Web, incluindo os usados pelo worm Nimda. O sensor de rede é capaz de identificar ataques e fornecer detalhes sobre os hosts afetados ou comprometidos para isolar a infecção Nimda.

Esses alarmes do sensor de rede IDS da Cisco disparam:

- Acesso WWW WinNT cmd.exe (SigID 5081)
- Decodificação dupla CGI do IIS (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 pelo nome. Eles veem uma série de alarmes observados quando Nimda tenta diferentes explorações para comprometer o alvo. Os alarmes identificam o endereço de origem dos hosts que foram comprometidos e que devem ser isolados da rede, limpos e corrigidos.

Cursos de ação recomendados

Siga estes passos para proteger contra o worm Nimda:

1. Aplique as atualizações mais recentes para o Microsoft Outlook, Outlook Express, Internet Explorer e IIS disponíveis na Microsoft .
2. Atualize o software de exploração de vírus com a correção mais recente para atenuar a propagação do vírus.**Nota:** Pode transferir a correção de vírus mais recente para proteger o seu computador contra infecções. Se o PC já foi infectado, este patch de vírus permite que você examine manualmente o disco rígido do PC e limpe a infecção da máquina.
3. Implante o Cisco IDS para atenuar a ameaça, conter a infecção e proteger os servidores.

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