Informações de referência de segurança

Conselhos e avisos de segurança localizam-se em http://www.cisco.com/go/psirt, junto com informações adicionais do PSIRT.

Melhores práticas

Melhorando a Segurança em Cisco Routers

Este documento é uma discussão informal de algumas configurações CISCO que os administradores de rede devem pensar em alterar em seus roteadores, especialmente nos roteadores de borda, a fim de melhorar a segurança. Este documento é sobre itens básicos de configuração do "boilerplate" que podem ser aplicados quase que universalmente nas redes IP e sobre alguns itens inesperados que devem ser considerados.

Fatos de criptografia de senhas do Cisco IOS

Uma origem que não é da Cisco lançou um programa para decodificar senhas de usuário (e outras senhas) em arquivos de configuração da Cisco. O programa não decodificará senhas definidas com o comando enable secret. A preocupação inesperada que este programa causou entre os clientes da Cisco levou-nos a suspeitar de que vários clientes estão usando a criptografia de senha da Cisco para obter um nível de segurança maior do que o projetado. Este documento explica o modelo de segurança por trás da criptografia de senha Cisco e as limitações de segurança desta criptografia

SAFE Blueprint da Cisco
O SAFE é um plano de segurança abrangente que permite que as empresas se envolvam com segurança no e-business. Usando uma abordagem modular que simplifica o design de segurança, a implementação e o gerenciamento à medida que as redes crescem e se transformam, o SAFE aprimora as redes desenvolvidas no Cisco AVVID (Arquitetura para Voz, Vídeo e Dados Integrados).

Estratégias para ataque e defesa, controle ou mitigação

Caracterizando e Rastreando Inundações de Pacote com Uso de Cisco Routers

> Os ataques de negação de serviço (DoS) são comuns na Internet. O primeiro passo em resposta a tal ataque é descobrir exatamente qual é o tipo de ataque. Muitos dos ataques de DoS usados com freqüência baseiam-se em inundações de pacotes de largura de banda elevada ou em outros fluxos de pacotes repetitivos. Este documento fornece informações para a compreensão e o rastreamento desses ataques.

Estratégias para combater o Vírus Nimda

Este índice fornece uma lista abrangente de todas as dicas técnicas e recomendações de mitigação para lidar com o vírus Nimda.

[Strategies to Combat the Code Red Worm]

Esse índice fornece uma lista abrangente de todas as dicas técnicas e recomendações de mitigação para lidar com o worm Código Vermelho.

[Estratégias de proteção contra ataques de DDoS (Distributed Denial of Service)]

Este white paper contém uma descrição técnica de como um possível ataque de DDoS ocorre e métodos sugeridos para usar o software Cisco IOS para se defender contra ele.

[Estratégias de proteção contra ataques de DDoS (Distributed Denial of Service) a UDP]

Este white paper contém uma descrição técnica de como um possível ataque de porta de diagnóstico UDP ocorre e métodos sugeridos para usar o software Cisco IOS para se defender contra ele.

[Estratégias para proteção contra ataques de recusa de serviços TCP SYN]

Este white paper contém uma descrição técnica de como um possível ataque TCP SYN ocorre e métodos sugeridos para usar o software Cisco IOS para se defender contra ele.

[O mais recente em ataques de negação de serviço: Descrição e informações de "murfing" para minimizar efeitos]
Note: O link acima aponta para um site externo que não é mantido pela Cisco Systems, Inc.

Ele fornece informações detalhadas sobre ataques de "smurf", com foco nos roteadores Cisco e como reduzir os efeitos desses ataques. Algumas informações são gerais e não estão relacionadas com o fornecedor de escolha específico de uma organização; no entanto, ele é escrito com foco no roteador Cisco. Este documento não é uma confirmação dos efeitos dos ataques de "smurf" em equipamentos de outros fornecedores; no entanto, ele contém informações sobre vários fornecedores.

Outros recursos

[Resposta de incidente de segurança de produto Cisco]

Este documento descreve os procedimentos de relatório de bug e resposta a incidentes especificamente, o que fazer se estiver sob um ataque ativo à segurança ou se acreditar que está prestes a sofrer um ataque, se tiver um problema de segurança com um produto Cisco, se desejar obter informações técnicas de segurança sobre um produto Cisco ou se tiver mais perguntas sobre uma questão de segurança com produto Cisco anunciada. A função da equipe de resposta a incidentes de segurança de produtos (PSIRT) da Cisco no tratamento de incidentes de segurança é explicada.
