Informations de référence de sécurité

Les bulletins de renseignements et les notices de Sécurité se trouvent chez http://www.cisco.com/go/psirt avec les informations complémentaires de l'équipe de réponse d'incident de sécurité du produit (PSIRT).

Meilleures pratiques

Amélioration de la Sécurité sur des Routeurs de Cisco

Ce document est une discussion informelle de quelques paramètres de configuration de Cisco que les administrateurs réseau devraient envisager changer sur leurs routeurs, particulièrement sur leurs routeurs interzone, afin d'améliorer la sécurité. Ce document est au sujet éléments de base, des de « zones fixes » de configuration qui s'appliquent presque universellement dans les réseaux IP, et au sujet de quelques éléments inattendus dont vous devriez se rendre compte.

Faits concernant le chiffrement de mot de passe dans Cisco IOS

Une source externe à Cisco a libéré un programme pour déchiffrer des mots de passe utilisateur (et d'autres mots de passe) dans des fichiers de configuration Cisco. Le programme ne déchiffrera pas des mots de passe définis avec la commande enable secret. Le souci inattendu que ce programme a entraîné parmi des clients de Cisco nous a menés à suspecter que beaucoup de clients comptent sur le cryptage de mot de passe de Cisco pour plus de sécurité qu'il avait été originalement conçu. Ce document explique le modèle de Sécurité derrière le cryptage de mot de passe de Cisco, et les limites de Sécurité de ce cryptage

Plan détaillé SÛR de Cisco

Le COFFRE-FORT est un plan détaillé complet de Sécurité qui permet à des organismes de s'engager sans risque dans le commerce électronique. Utilisant une approche modulaire qui simplifie la conception en matière de sécurité, le lancement, et la Gestion pendant que les réseaux se développent et changent, le COFFRE-FORT améliore des réseaux établis sur le Cisco AVVID (architecture pour la Voix, le vidéo et les données intégrées).

Stratégies pour la défense, le cheminement ou la réduction d'attaque

Caractérisation et suivi des inondations de paquets à l'aide de routeurs Cisco

Les attaques de déni de service sont courantes sur Internet. La première étape en réponse à une telle attaque est de découvrir exactement quel tri d'attaque c'est. Plusieurs des attaques de déni de service utilisées généralement sont basées sur l'envoi massif de paquets de bande passante élevée, ou sur d'autres flux répétitifs de paquets. Ce document fournit la vue dans comprendre et tracer ces attaques.

Stratégies pour combattre le virus Nimda

Cet index fournit une liste complète de tous les conseils techniques et recommandations de réduction pour avoir affaire avec le virus Nimda.

Stratégies pour combattre le ver Code Red

Cet index fournit une liste complète de tous les conseils techniques et recommandations de réduction pour avoir affaire avec le ver Code Red.

Stratégies de protection contre les attaques par déni de service distribuées

Ce Livre Blanc contient une description technique de la façon dont une attaque DDoS potentielle se produit et a suggéré des méthodes pour l'usage du logiciel de Cisco IOS pour défendre contre lui.

Stratégies à protéger contre des attaque de refus de service sur un port de diagnostic d'UDP

Ce Livre Blanc contient une description technique de la façon dont une attaque diagnostique de

port d'UDP potentiel se produit et a suggéré des méthodes pour l'usage du logiciel de Cisco IOS pour défendre contre lui.Stratégies à protéger contre des attaques par déni de service de synchronisation de TCP

Ce Livre Blanc contient une description technique de la façon dont une attaque potentielle de synchronisation de TCP se produit et a suggéré des méthodes pour l'usage du logiciel de Cisco IOS pour défendre contre lui.Le plus en retard dans les attaques par déni de service : Description et informations de « Smurfing » pour réduire des effets

Remarque: Les points ci-dessus de lien à un site externe qui n'est pas mis à jour par Cisco Systems, Inc.

Il fournit aux informations en profondeur concernant des attaques de « smurf », un foyer sur des Routeurs de Cisco et comment réduire les effets de ces attaques. Quelques informations sont générales et non connexes au constructeur particulier d'une organisation de choix ; cependant, on lui écrit avec un foyer de routeur de Cisco. Ce document n'est pas une confirmation des effets des attaques de « smurf » sur l'autre matériel de constructeurs ; cependant, il contient des informations sur de divers constructeurs.

D'autres ressources

Résolution d'incidents de sécurité des produits CiscoCe document décrit l'enregistrement de bogue et les procédures de réponse d'incident - spécifiquement, quoi faire si vous êtes soumise à l'attaque active contre la sécurité ou vous croyez que vous êtes sur le point d'être attaquée, si vous avez un problème de Sécurité avec un produit de Cisco, si vous voulez obtenir les informations de sécurité techniques au sujet d'un produit de Cisco, ou si vous avez des questions supplémentaires au sujet d'un problème de sécurité annoncé avec un produit de Cisco. Le rôle de l'équipe de résolution d'incidents de sécurité des produits Cisco (PSIRT) en manipulant des incidents de sécurité est expliqué.