Informations de référence de sécurité

Les avis et notifications de sécurité sont disponibles à l'adresse http://www.cisco.com/go/psirt, ainsi que des informations complémentaires de l'équipe de réponse aux incidents de sécurité des produits (PSIRT).

Meilleures pratiques

Amélioration de la sécurité sur les routeurs 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 traite des éléments de configuration de base, « standard », qui sont presque universellement applicables dans les réseaux IP, et de quelques éléments inattendus dont vous devriez être conscient.

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 SAFE de Cisco

SAFE est un plan de sécurité complet qui permet aux entreprises de s'engager en toute sécurité dans le commerce électronique. Grâce à une approche modulaire qui simplifie la conception, le déploiement et la gestion de la sécurité à mesure que les réseaux se développent et évoluent, SAFE améliore les réseaux basés sur Cisco AVVID (Architecture for Voice, Video and Integrated Data).

Stratégies de défense, de suivi ou d'atténuation des attaques

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 pour répondre à une telle attaque consiste à déterminer exactement quel type d'attaque il s'agit. 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 des informations sur la compréhension et le suivi de ces attaques.

Stratégies de lutte contre le virus Nimda

Cet index fournit une liste complète de tous les conseils techniques et recommandations d'atténuation pour traiter le virus Nimda.

Stratégies de lutte contre le ver Code Red

Cet index fournit une liste complète de tous les conseils techniques et recommandations d'atténuation pour traiter le ver Code Red.

Stratégies de protection contre les attaques par déni de service distribuées

Ce livre blanc contient une description technique de la manière dont une attaque DDoS potentielle se produit et des méthodes suggérées pour l'utilisation du logiciel Cisco IOS afin de se défendre contre cette attaque.

Stratégies de protection contre les attaques par déni de service des ports de diagnostic UDP

Ce livre blanc contient une description technique de la manière dont se produit une attaque potentielle du port de diagnostic UDP et des méthodes suggérées pour utiliser le logiciel Cisco IOS afin de se défendre contre cette attaque.

Stratégies de protection contre les attaques par déni de service SYN TCP

Ce livre blanc contient une description technique de la manière dont une attaque TCP SYN potentielle se produit et des méthodes suggérées pour utiliser le logiciel Cisco IOS afin de se défendre contre cette attaque.

Dernières attaques par déni de service : description et informations sur le « Schtroumppage » pour minimiser les effets
Remarque : le lien ci-dessus pointe vers un site externe qui n'est pas géré par Cisco Systems, Inc.

Il fournit des informations détaillées sur les attaques « schtroumpfs », en mettant l'accent sur les

routeurs Cisco et sur la manière de réduire les effets de ces attaques. Certaines informations sont générales et ne sont pas liées au fournisseur choisi par l'entreprise. Toutefois, elles sont rédigées en mettant l'accent sur les routeurs Cisco. Ce document n'est pas une confirmation des effets des attaques « schtroumpfs » sur l'équipement d'autres fournisseurs ; cependant, il contient des informations sur divers fournisseurs.

Autres ressources

[Réponse aux incidents de sécurité des produits Cisco]

Ce document décrit les procédures de signalement de bogues et de réponse aux incidents. En particulier, ce qu'il faut faire si vous subissez une attaque de sécurité active ou si vous pensez que vous êtes sur le point d'être attaqué, si vous rencontrez un problème de sécurité avec un produit Cisco, si vous souhaitez obtenir des informations techniques sur la sécurité d'un produit Cisco ou si vous avez des questions supplémentaires sur un problème de sécurité annoncé avec un produit Cisco. Le rôle de l'équipe Cisco Product Security Incident Response Team (PSIRT) dans la gestion des incidents de sécurité est expliqué.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.