Todos los avisos y asesores de seguridad se encuentran disponibles en http://www.cisco.com/go/psirt, junto con información adicional del Equipo de respuestas ante problemas de seguridad de productos (PSIRT).

Mejores medidas

Mejora de seguridad de los routers de Cisco

Este documento es un debate informal sobre algunos ajustes de la configuración de Cisco que los administradores de red deben intentar cambiar en sus routers, especialmente en los routers de borde, a fin de mejorar la seguridad. Este documento es sobre la configuración básica de los "textos modelo" que pueden aplicarse casi universalmente a las redes IP y sobre algunos ítems inesperados de los cuáles debe estar advertido

Aspectos del encripción de contraseña de IOS de Cisco

Una fuente que no es Cisco ha lanzado un programa para descifrar contraseñas de usuarios (y otras contraseñas) en archivos de configuración Cisco. El programa no descifrará contraseñas definidas con el comando enable secret. EIEE 'El interés inesperado que este programa ha causado entre los clientes de Cisco nos ha llevado a sospechar que muchos clientes confían en que el encripción de contraseñas de Cisco les brindará mayor seguridad de la que fue diseñado para brindar. Este documento explica el modelo de seguridad detrás de la encripción de contraseñas de Cisco, y las limitaciones de seguridad de ese cifrado

Plano SAFE de Cisco

La CAJA FUERTE es un plan general de seguridad completo que permite a las organizaciones para enganchar con seguridad al comercio electrónico. Mediante el uso de un enfoque modular que simplifica el diseño, el desarrollo y la administración de la seguridad a medida que las redes crecen y cambian, SAFE mejora las redes construidas con AVVID (Arquitectura para voz, video y datos integrados) de Cisco.

Estrategias de defensa, seguimiento o mitigación

Caracterización y seguimiento de la inundación de paquetes usando routers de Cisco Los ataques de rechazo de servicio (DoS) son frecuentes en Internet. El primer paso para responder a tal ataque es averiguar de qué tipo de ataque se trata exactamente. La mayoría de los ataques DOS que se utilizan comúnmente están basados en inundaciones de paquetes de ancho de banda alto o en otras secuencias de paquetes repetitivas. Este documento permite comprender y realizar un seguimiento de estos ataques.**Estrategias para luchar contra el virus Nimda**Este índice proporciona un anuncio completo de todos los consejos técnicos y recomendaciones de la mitigación para tratar del virus NIMDA. **Estrategias para combatir el gusano de código rojo**Este índice ofrece un listado completo de todos los consejos técnicos y recomendaciones de mitigación para combatir al gusano de “código rojo”. **Estrategias de protección contra ataques de la negación de servicio distribuida (DDoS)**Este White Paper contiene una descripción técnica de cómo ocurre un ataque DDoS potencial y los métodos sugeridos para usar el Cisco IOS Software para defender contra él.**Estrategias para la protección contra ataques de denegación de servicio en el puerto de diagnóstico UDP**Este White Paper contiene una descripción técnica de cómo ocurre un establecimiento de puerto de diagnóstico del potencial UDP y los métodos sugeridos para usar el Cisco IOS Software para defender contra él. **Estrategias para protegerse de los ataques de denegación de servicio SYN TCP**Este White Paper contiene una descripción técnica de cómo ocurre un Ataque SYN del potencial TCP y los métodos sugeridos para usar el Cisco IOS Software para defender contra él.**El más último de los establecimientos de rechazo del servicio: Descripción e información del “Smurfing” para minimizar**

los efectos

Nota: Las puntas antedichas del link a un sitio externo que no es mantenido por Cisco Systems, Inc.

Otros recursos

Respuesta ante problemas de seguridad de productos Cisco

Este documento describe los informes de los errores de funcionamiento y los procedimientos de respuesta a incidentes; específicamente, qué debe hacer si está sufriendo un ataque de seguridad activo o si cree que está por sufrir un ataque, si tiene un problema de seguridad con un producto de Cisco, si desea obtener información sobre seguridad técnica para un producto de Cisco o si tiene más preguntas sobre un problema de seguridad anunciado de un producto de Cisco. El papel del equipo de la respuesta a incidente de seguridad de producto de Cisco (PSIRT) en la manipulación de los incidentes de seguridad se explica.