Informazioni di riferimento sulla sicurezza

Gli avvisi e i consigli sulla sicurezza sono disponibili all'indirizzo http://www.cisco.com/go/psirt insieme a ulteriori informazioni del team PSIRT (Product Security Incident Response Team).

Procedure ottimali

Miglioramento della sicurezza sui router Cisco

Questo documento è una discussione informale su alcune impostazioni di configurazione di Cisco che gli amministratori di rete dovrebbero prendere in considerazione per modificare sui propri router, soprattutto sui router di confine, per migliorare la sicurezza. Questo documento tratta dei componenti di configurazione di base "standard" che sono quasi universalmente applicabili alle reti IP e di alcuni elementi imprevisti di cui è necessario essere consapevoli.

Informazioni sulla crittografia delle password di Cisco IOS

Un programma realizzato da una fonte esterna a Cisco permette di decriptare le password degli utenti (e altre password) nei file di configurazione Cisco. Il programma non decripta le password impostate con il comando enable secret. L'inaspettata preoccupazione che questo programma ha causato tra i clienti Cisco ci ha fatto capire quanto i clienti facciano affidamento sulla crittografia delle password Cisco per avere una sicurezza maggiore di quanto non fosse stato inizialmente progettato. In questo documento viene spiegato il modello di sicurezza sottostante alla crittografia delle password Cisco e i limiti per la sicurezza di tale crittografia

Progetto SAFE di Cisco
SAFE è un piano di sicurezza completo che consente alle organizzazioni di impegnarsi in modo sicuro nell'e-business. Utilizzando un approccio modulare che semplifica la progettazione, il rollout e la gestione della sicurezza con la crescita e il cambiamento delle reti, SAFE migliora le reti basate su Cisco AVVID (Architecture for Voice, Video and Integrated Data).

Strategie per la difesa, la localizzazione o la mitigazione degli attacchi

Caratterizzazione e traccia delle inondazioni di pacchetti tramite router Cisco

> Gli attacchi DoS (Denial of Service) sono comuni su Internet. Il primo passo per rispondere a un attacco di questo tipo è scoprire esattamente che tipo di attacco è. Molti degli attacchi DoS comunemente utilizzati sono basati su pacchetti a larghezza di banda elevata o su altri flussi ripetitivi di pacchetti. Questo documento offre informazioni dettagliate sulla comprensione e la traccia di questi attacchi.

Strategie per combattere il virus Nimda

Questo indice fornisce un elenco completo di tutti i suggerimenti tecnici e le raccomandazioni di mitigazione per la gestione del virus Nimda.

[Strategie per combattere il verme rosso]

Questo indice fornisce un elenco completo di tutti i suggerimenti tecnici e le raccomandazioni di mitigazione per la gestione del worm Code Red.

[Strategie di protezione dagli attacchi Distributed Denial of Service (DDoS)]

Questo white paper contiene una descrizione tecnica di come si verifica un potenziale attacco DDoS e suggerisce i metodi per l'utilizzo del software Cisco IOS per difendersi da tale attacco.

[Strategie di protezione dagli attacchi Denial of Service delle porte di diagnostica UDP]

Questo white paper contiene una descrizione tecnica di come si verifica un potenziale attacco alla porta diagnostica UDP e dei metodi consigliati per l'utilizzo del software Cisco IOS per proteggersi da tale attacco.

[Strategie di protezione dagli attacchi Denial of Service TCP SYN]

Questo white paper contiene una descrizione tecnica di come si verifica un potenziale attacco TCP SYN e suggerisce i metodi per l'utilizzo del software Cisco IOS per difendersi da esso.

[Gli ultimi attacchi Denial of Service: Descrizione e informazioni per ridurre al minimo gli effetti]
Nota: Il link riportato sopra fa riferimento a un sito esterno non gestito da Cisco Systems, Inc.

Fornisce informazioni approfondite sugli attacchi "smurf", con particolare attenzione ai router Cisco e a come ridurre gli effetti di questi attacchi. Alcune informazioni sono generali e non sono correlate al fornitore scelto dall'organizzazione; tuttavia, è scritto con un router Cisco attivo. Il presente documento non conferma gli effetti degli attacchi "smurf" sulle apparecchiature di altri fornitori; tuttavia, contiene informazioni sui vari fornitori.

Altre risorse

[Cisco Product Security - Risposta agli incidenti]

Questo documento descrive le procedure di segnalazione dei bug e di risposta agli incidenti - in particolare, cosa fare se si è sotto un attacco alla sicurezza attivo o si ritiene di essere sul punto di essere attaccati, se si ha un problema di sicurezza con un prodotto Cisco, se si desidera ottenere informazioni tecniche di sicurezza su un prodotto Cisco o se si hanno domande aggiuntive su un problema di sicurezza annunciato relativo a un prodotto Cisco. Viene spiegato il ruolo del Cisco Product Security Incident Response Team (PSIRT) nella gestione degli incidenti relativi alla sicurezza.
