Protezione da attacchi Denial of Service delle porte di diagnostica UDP

Sommario

Introduzione

Sui provider di servizi Internet è presente un potenziale attacco Denial of Service destinato ai dispositivi di rete.

- **Attacco alla porta di diagnostica UDP (User Datagram Protocol):** Un mittente trasmette un volume di richieste per i servizi di diagnostica UDP sul router. In questo modo, tutte le risorse CPU verranno utilizzate per soddisfare le richieste false.

In questo documento viene descritto come si verifica il potenziale attacco alla porta diagnostica UDP e vengono suggeriti i metodi da utilizzare con il software Cisco IOS® per proteggersi da tale attacco.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. Alcuni dei comandi

menzionati in questo documento sono disponibili solo a partire dal software Cisco IOS versione 10.2(9), 10.3(7) e 11.0(2), e tutte le versioni successive. Questi comandi sono quelli predefiniti del software Cisco IOS versione 12.0 e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Descrizione del problema

L'attacco alla porta di diagnostica UDP

Per impostazione predefinita, il router Cisco dispone di una serie di porte diagnostiche abilitate per alcuni servizi UDP e TCP. Questi servizi includono echo, chargen e discard. Quando un host si collega a queste porte, viene utilizzata una piccola quantità di capacità della CPU per soddisfare queste richieste.

Se un singolo dispositivo attaccante invia un'ampia quantità di richieste con indirizzi IP di origine diversi, casuali e fasulli, è possibile che il router Cisco si blocchi e rallenti o guasti.

La manifestazione esterna del problema include un messaggio di errore completo della tabella del processo (`%SYS-3 NOPROC`) o un utilizzo della CPU molto elevato. Il comando exec **show process** mostra molti processi con lo stesso nome, ad esempio "UDP Echo".

Difesa dagli attacchi direttamente ai dispositivi di rete

Disabilita porte di diagnostica UDP

Tutti i dispositivi di rete dotati di servizi diagnostici UDP e TCP devono essere protetti da un firewall o avere i servizi disabilitati. Per un router Cisco, ciò può essere realizzato utilizzando questi comandi di configurazione globale.

```
no service udp-small-servers
no service tcp-small-servers
```

Vedere l'Appendice per ulteriori informazioni su questi comandi. I comandi sono disponibili a partire dal software Cisco IOS versione 10.2(9), 10.3(7) e 11.0(2) e da tutte le versioni successive. Questi comandi sono quelli predefiniti del software Cisco IOS versione 12.0 e successive.

Prevenzione di attacchi involontari da parte della rete

Poiché un meccanismo primario di attacchi Denial of Service è la generazione di traffico proveniente da indirizzi IP casuali, Cisco consiglia di filtrare il traffico destinato a Internet. Il concetto di base è quello di eliminare i pacchetti con indirizzi IP di origine non validi quando entrano in Internet. Ciò non impedisce l'attacco Denial of Service alla rete. Tuttavia, aiuta le parti attaccate escludere la vostra posizione come fonte dell'aggressore. Impedisce inoltre l'utilizzo

della rete per questa classe di attacchi.

Impedisci la trasmissione di indirizzi IP non validi

Filtrando i pacchetti sui router che connettono la rete a Internet, è possibile consentire solo ai pacchetti con indirizzi IP di origine validi di uscire dalla rete e accedere a Internet.

Ad esempio, se la rete è costituita dalla rete 172.16.0.0 e il router si connette all'ISP utilizzando un'interfaccia FDDI0/1, è possibile applicare l'elenco degli accessi nel modo seguente:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log [1]

interface Fddi 0/1
ip access-group 111 out
```

[1]L'ultima riga dell'elenco degli accessi determina se è presente traffico con un indirizzo di origine non valido che entra in Internet. Questo aiuta a individuare la fonte dei possibili attacchi.

Impedisci ricezione di indirizzi IP non validi

Per gli ISP che forniscono servizi alle reti terminali, Cisco consiglia di convalidare i pacchetti in arrivo dai client. A tale scopo, è possibile utilizzare i filtri pacchetti in ingresso sui router di confine.

Ad esempio, se i client hanno questi numeri di rete connessi al router tramite un'interfaccia FDDI denominata "FDDI 1/0", è possibile creare questo elenco degli accessi.

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface Fddi 1/0
ip access-group 111 in
```

Nota: l'ultima riga dell'elenco degli accessi determina se è presente traffico con un indirizzo di origine non valido che entra in Internet. Questo aiuta a individuare la fonte del possibile attacco.

Appendice Descrizione dei server di piccole dimensioni

I server di piccole dimensioni sono server (daemon, in linguaggio UNIX) eseguiti nel router e utili per la diagnostica. Pertanto, sono attivati per default.

I comandi per i piccoli server TCP e UDP sono:

- **service tcp-small-servers**
- **service udp-small-servers**

Se non si desidera che il router fornisca servizi non di routing, disattivarli (usando la forma **no** dei comandi precedenti).

I piccoli server TCP sono:

- **Eco** (**Echo**) - Eco qualsiasi testo digitato. Digitare il comando **telnet x.x.x.x echo** da visualizzare.
- **Caricato (Chargen**) - Genera un flusso di dati ASCII. Digitare il comando **telnet x.x.x.x** a **carico**.
- **Ignora (Discard**) - Elimina qualsiasi testo digitato. Digitare il comando **telnet x.x.x.x ignorare** per visualizzare.
- **Daytime** - Restituisce la data e l'ora di sistema, se corrette. È corretto se si esegue NTP o se la data e l'ora sono state impostate manualmente dal livello di esecuzione. Digitare il comando **telnet x.x.x.x daytime** per visualizzarlo.

I piccoli server UDP sono:

- **Eco**: echeggia il payload del datagramma inviato.
- **Elimina**: attiva automaticamente il datagramma inviato.
- **Caricamento**: attiva il datagramma inviato e risponde con una stringa di 72 caratteri ASCII terminata con CR+LF.

Nota: quasi tutte le caselle UNIX supportano i server di piccole dimensioni elencati in precedenza. Il router offre anche il servizio finger e il servizio bootp in linea asincrona. Questi possono essere disattivati in modo indipendente con i comandi globali di configurazione **no service finger** e **no ip bootp server**, rispettivamente.

Informazioni correlate

- Software Cisco IOS
- Supporto tecnico – Cisco Systems