Prevenzione di frame jumbo ICMP sugli switch gestiti serie SG200/300

Obiettivo

In questo documento viene spiegato perché gli switch serie SG200 e SG300 impediscono la trasmissione di alcuni frame jumbo ICMP e ne consentono il passaggio da altri. Questo articolo mostra quali problemi sono causati dai frame jumbo ICMP. L'articolo spiega anche cos'è un attacco Denial of Service (DoS) e come si relaziona ai frame jumbo ICMP.

Dispositivi interessati

SG200
•SG300

Frame jumbo ICMP sullo switch

Di seguito vengono spiegati i frame jumbo e il motivo per cui i frame jumbo ICMP non sono consentiti sugli switch serie SG200 e SG300.

Frame jumbo

Gli switch Gigabit Ethernet (serie SG200 e SG300) e Fast Ethernet (serie SF200) supportano i frame jumbo. I frame jumbo sono frame Ethernet estesi con dimensioni comprese tra 1.518 byte standard e 9.000 byte. In questo modo, i frame jumbo aumentano la velocità di trasferimento dei dati portando più dati per frame, riducendo l'overhead delle intestazioni.

Protocollo ICMP (Internet Control Message Protocol)

ICMP è un protocollo a livello di rete che fa parte della suite di protocolli Internet e genera messaggi ICMP in risposta a errori nel datagramma IP o a scopi di diagnostica o routing. Gli errori ICMP vengono sempre segnalati all'indirizzo IP di origine del datagramma originale. Sebbene questo protocollo sia molto importante per garantire la corretta distribuzione dei dati, può essere sfruttato da utenti malintenzionati per la conduzione di diversi attacchi

Denial of Service (DoS).

Gli attacchi DoS rendono le risorse di rete e server non disponibili o non rispondono agli utenti legittimi attraverso reti inondanti con traffico falso. Gli attacchi DoS con la forza bruta consumano il server e la larghezza di banda della rete inondando il server con un traffico eccessivo. Di seguito sono elencati i tipi più comuni di attacchi DoS che utilizzano ICMP.

· ICMP Ping Flood Attack - In un attacco Ping Flood di tipo ICMP, l'attacco invia un numero enorme di pacchetti ping al sistema di destinazione, generalmente tramite il comando ping inviato dall'host. In questo modo il sistema attaccato non può rispondere al traffico legittimo.

· ICMP Smurf Attack - Un ICMP Smurf Attack invia al computer della vittima pacchetti ping falsificati. Si tratta di pacchetti modificati che contengono un indirizzo IP falsificato della vittima di destinazione. In questo modo la disinformazione viene trasmessa a tutti gli host della rete locale. Tutti questi host rispondono con una risposta al sistema di destinazione, che è poi saturo di quelle risposte.Se ci sono molti host nelle reti usate, la vittima sarà effettivamente spoofed da una grande quantità di traffico.

Nota: lo spoofing IP si riferisce a un pacchetto IP con un indirizzo IP di origine contraffatto, allo scopo di nascondere le informazioni del mittente.

· Ping of Death (Ping della morte) - In un ping di attacco mortale, l'attaccante invia alla vittima un pacchetto di richiesta echo ICMP più grande della dimensione massima del pacchetto IP di 65.536 byte. Poiché il pacchetto di richiesta echo ICMP ricevuto è più grande delle dimensioni del pacchetto IP normale, deve essere frammentato. Di conseguenza, la vittima non è in grado di ricomporre i pacchetti, quindi il sistema operativo si blocca o si riavvia.

· ICMP Nuke Attack - In questo tipo di attacco, le armi nucleari vengono inviate alla vittima attraverso un pacchetto ICMP con messaggi di destinazione irraggiungibile che sono di tipo 3. Il risultato di questo attacco è che il sistema di destinazione interrompe le comunicazioni con le connessioni esistenti.

Sugli switch serie SG200 e SG300, la funzione di prevenzione della negazione del servizio consente ai manager di rete di configurare il blocco di alcuni pacchetti ICMP. Per impostazione predefinita, alcuni frame jumbo ICMP sono bloccati perché molti attacchi alla rete, ad esempio i DoS, utilizzano l'ICMP. Per motivi di sicurezza, i firewall di questi switch bloccano i frame jumbo ICMP. Ciò determina la necessaria frammentazione ICMP e il messaggio DF impostato non raggiunge il mittente. Il mittente quindi non riceve informazioni per inviare i pacchetti con dimensioni inferiori né riceve una conferma TCP che i pacchetti sono stati inviati correttamente. Successivamente, il mittente continua a inviare di nuovo il

frame con le stesse dimensioni, ma non raggiunge mai la destinazione, creando una condizione nota come "buco nero".

Usare l'utility di configurazione Web per configurare i frame jumbo, scegliere Gestione porte > Impostazioni porta e scegliere Sicurezza > Prevenzione negazione del servizio > Impostazioni della suite di sicurezza per configurare la prevenzione DoS.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).