Falla nel kernel: sistemi Linux a rischio attacco DoS

Giu 18, 2019 Marco Schiaffino Emergenze, In evidenza, News, RSS, Vulnerabilità 0

TCP SACK PANIC permette di portare un attacco in remoto che porta al blocco del sistema a livello kernel. Allarme per i server aziendali e i sistemi cloud.

L'hanno battezzata **TCP SACK PANIC** ed è una falla nella gestione del protocollo di connessione che potrebbe causare parecchi guai in ambiti aziendali e (soprattutto) nei sistemi cloud, per la maggioranza affidati a sistemi Linux.

I tre bug (CVE-2019-11477, CVE-2019-11478 e CVE-2019-11479) interessano il kernel e di conseguenza coinvolge **tutte le distro Linux** e le piattaforme derivate (per esempio quella **Amazon** di **AWS**) basate sul sistema open source. Lo scenario, spiegano i ricercatori, è quello di un attacco remoto che potrebbe mettere in un attimo K.O. i sistemi.

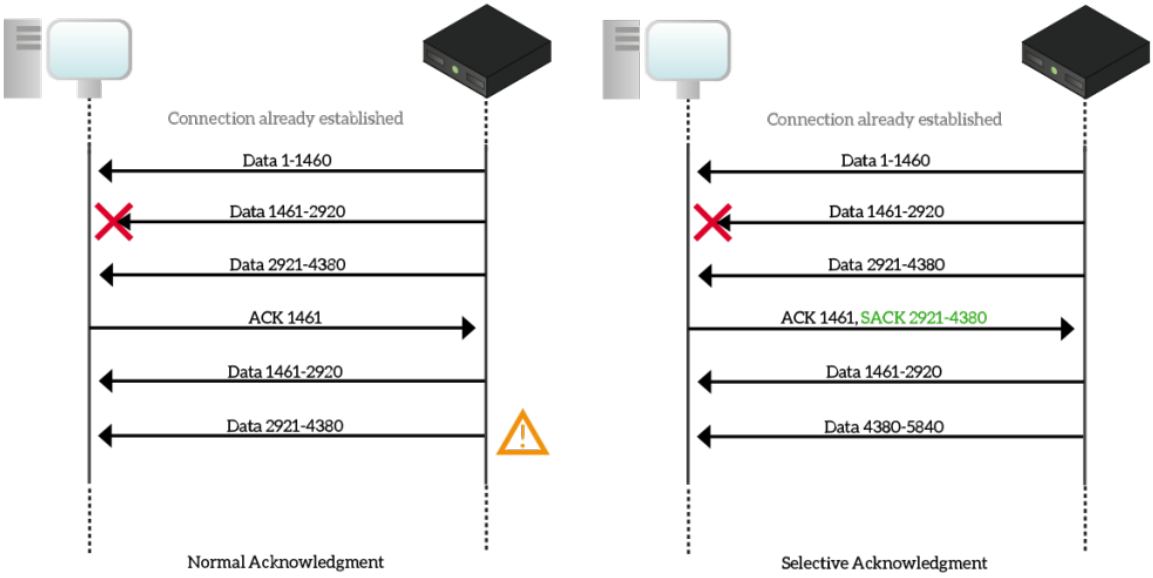
Ma di cosa stiamo parlando esattamente? SACK (Selective Acknowledgements) è un meccanismo che permette di **ottimizzare la trasmissione dei pacchetti nelle connessioni TCP** (Transmission Control Protocol) utilizzate normalmente per le comunicazioni su Internet.

Il protocollo TCP, tra le sue caratteristiche, ha quella di prevedere un sistema di verifica dell'integrità delle comunicazioni. In pratica, se una parte dei pacchetti inviati non raggiunge il destinatario, questi frammenti vengono ritrasmessi.

Normalmente, in caso di perdita di una parte dei dati, la

trasmissione viene ripetuta integralmente a partire dal primo segmento mancante.

Come viene spiegato esaurientemente in questo report di **Red Hat**, SACK permette di **individuare con precisione i pacchetti andati persi nella trasmissione** e fare in modo che solo quelli effettivamente mancanti debbano essere trasmessi di nuovo. Come risultato, l'utilizzo di SACK consente di effettuare le comunicazioni con una maggiore efficienza e velocità.



Quello che i ricercatori hanno scoperto, è come sia possibile utilizzare una trasmissione TCP per mandare in "cortocircuito" il sistema semplicemente sovraccaricando il **Socket Buffer (SKB)** che nei sistemi Linux si occupa di gestire le code di frammenti nei collegamenti TCP.

Per farlo, un pirata dovrebbe avviare una connessione TCP in cui le dimensioni dei segmenti (**Maximum Segment Size o MSS**) siano impostate al valore minimo (48 byte) e trasmettere una sequenza particolare di pacchetti SACK al bersaglio.

La procedura, secondo quanto riportano gli sviluppatori, innescherebbe il blocco del Socket Buffer e, a cascata, dell'intero sistema operativo.

Gli aggiornamenti del kernel sono già disponibili e (si spera)

in corso di aggiornamento per tutte le macchine interessate.

Condividi l’articolo

Symantec subisce un attacco a un suo lab australiano Più di 900.000 utenti colpiti da malware diffusi da video giochi contraffatti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/18/falla-nel-kernel-sistemi-linux-a-rischio-attacco-dos/