bicom SYSTEMS

MANTIENI SICURO IL TUO SISTEMA

DATASHEET

sipPROT

sipPROT

sipPROT è un modulo di PBXware e SERVERware che fornisce protezione dagli attacchi SIP. Tentativi di effrazione e gli attacchi Denial of Service sono abbastanza frequenti e rappresentano una minaccia imprevedibile. I sistemi PBX VoIP non protetti sono molto sensibili a questo tipo di attacchi. Il più comune di questi tipi di attacchi alla rete sono i tempi di inattività del servizio VOIP, problemi di qualità delle chiamate dovuti a una rete sovraccarica e frodi dirette a causa dell'instabilità della rete. Lo scopo principale di sipPROT è prevenire questi attacchi.

FILTRI E BLOCCHI DELL'INDIRIZZO IP

Whitelist List: L'elenco degli indirizzi IP che non verranno in nessun caso bloccati da sipPROT. Gli indirizzi IP nella whitelist vengono aggiunti manualmente dall'amministratore.

Blacklist: L'elenco degli indirizzi IP che verranno sempre bloccati da sipPROT. Gli indirizzi IP nella blacklist vengono aggiunti manualmente, dall'amministratore o automaticamente dal sipPROT, a seconda di quanto impostato nel file di configurazione sipprot.conf

Whitelist/Blacklist Management: Gestione whitelist/blacklist tramite modulo ipset se presente nel sistema.

REGISTRAZIONE E NOTIFICHE

Logging & Notifiche
E' possibile configurare il sipPROT per inviare notifiche che informano l'amministratore dei potenziali attacchi.

PROTEZIONE DEL TRAFFICO SIP

Protocolli TCP/UDP
sipPROT monitora il traffic SIP su entrambi i protocolli TCP e UDP.

Gestione Dinamica della Blacklist
sipPROT inserisce temporaneamente qualsiasi indirizzo IP nella Blacklist nel caso in cui tenti di registrarsi più volte sul PBXware in un breve lasso temporale. Dopo la scadenza del periodo predefinito, l'indirizzo IP verrà rimosso automaticamente dalla Black List Dinamica.

Protezione SIP REGISTER
La protezione SIP REGISTER blocca dinamicamente un indirizzo IP se un numero di registrazioni SIP errate supera la soglia configurata (hit_count) entro un determinato periodo di monitoraggio (monit_period). Il parametro di configurazione block_threshold definisce quante volte un indirizzo IP verrà bloccato dinamicamente prima di essere inserito nella Blacklist statica.

Protezione SIP Invite
La limitazione della frequenza SIP INVITE non protegge completamente da un attacco SIP INVITE, limita semplicemente l'impatto dell'attacco DoS.
Quando un numero di SIP INVITE simultanei supera il limite configurato,verrà inviata una notifica all'amministratore del sistema. Spetta all'amministratore di sistema decidere se aggiungere permanentemente l'indirizzo IP di origine alla Blacklist o aumentare il rate_limit se gli INVITES provengono da un indirizzo IP noto.

Protezione SIP Scanners
Il generatore di report consente agli utenti di creare un report dai dati storici in base ai criteri preferiti.

Protezione TFTP
La protezione TFTP ti consente di proteggere i tuoi server dagli attacchi di forza bruta TFTP utilizzando il limite di velocità. In un esempio di impostazioni predefinite, se SIPprot rileva più di 100 richieste tftp da un singolo IP in un minuto,le ulteriori richieste da quell' IP sarnò limitate 10/minuto.

Protezione DNS : Protezione DNS ti consente di proteggere i tuoi server dalla recente vulnerabilità glibc (CVE-2015-7547) che colpisce i client DNS.
Per abilitare/disabilitare questo tipo di protezione, usare il dns_protection config parameter.

bicom
SYSTEMS

Via M. Curie 3, Castelfiorentino 50051 (FI)
info@bicomsystems.it
+39 0571 1661119

www.bicomsystems.it