

Eventi di autenticazione VPN RSA ad accesso sicuro con indirizzi server AAA locali al collegamento

Sommario

Problema

Durante la verifica della funzionalità VPN di Accesso remoto sicuro, vengono registrati eventi di autenticazione eccessivi per le identità che non esistono nell'organizzazione tenant. I registri di autenticazione mostrano oltre 10.000 eventi di autenticazione VPN AAA in un periodo di 24 ore, contenenti errori AAA come "AAALOG_SERVICE_DOWN" e "AAALOG_SERVER_DOWN". Questi messaggi di errore fanno riferimento agli indirizzi locali del collegamento 169.254.x.x come server AAA, che non sono configurati nel tenant.

Di seguito sono riportati alcuni esempi di errori specifici osservati nei registri:

```
AAALOG_SERVICE_DOWN  
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>
```

```
AAALOG_SERVER_DOWN  
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

L'attività sembra essere costituita da ripetuti tentativi di autenticazione basati su RADIUS contro l'FQDN della VPN ad accesso sicuro, che creano un eccessivo disturbo del registro e sollevano preoccupazioni sulla scansione esterna o sul potenziale abuso del servizio VPN.

Ambiente

- Piattaforma Cisco Secure Access
- Profilo VPN di Accesso remoto inizialmente configurato senza autenticazione certificato

- Autenticazione basata su RADIUS configurata per RSA VPN
- Configurazione tenant VPN pubblico con profili VPN individuabili

Risoluzione

La risoluzione implicava la comprensione del comportamento del flusso di autenticazione e l'implementazione dell'autenticazione basata su certificati come strategia di mitigazione.

Spiegazione tecnica dei comportamenti osservati

Gli eventi di autenticazione eccessivi si verificano a causa di motivi tecnici descritti nelle sezioni seguenti.

Flusso di autenticazione senza requisiti certificato

Quando l'autenticazione dei certificati è disabilitata e viene utilizzata l'autenticazione VPN per Autorità registrazione basata su RADIUS, il sistema registra i tentativi di "autorizzazione non riuscita" poiché il sistema controlla innanzitutto l'identità del nome utente in base al database degli utenti sincronizzati in Secure Access e registra l'evento "autorizzazione non riuscita". Questi eventi sono attesi come prima linea di difesa, ma possono produrre un notevole rumore di registro quando gli attori esterni tentano l'autenticazione.

Utilizzo indirizzo locale del collegamento

Gli indirizzi 169.254.x.x visualizzati nei log sono indirizzi di collegamento interno/locale utilizzati dall'headend VPN per l'autorizzazione delle sessioni in ingresso. Questi indirizzi rappresentano il comportamento del sistema interno piuttosto che la configurazione errata dei server AAA nel tenant.

Rilevamento profilo VPN

Quando viene configurato un ID tenant VPN pubblico, i profili VPN vengono elencati nell'elenco a discesa dell'interfaccia utente, che consente agli attori esterni di individuare più facilmente i profili pubblici e di utilizzarli per i tentativi di autenticazione.

Fasi di mitigazione immediata

1.- Configurare l'autenticazione basata sui certificati. Modificare il profilo VPN Autorità registrazione per richiedere l'autenticazione basata su certificati. Quando è necessaria l'autenticazione dei certificati, Secure Access esegue un controllo dei certificati in una fase precedente del flusso di autenticazione. Se il certificato è mancante, il sistema genera un errore prima del flusso di autenticazione standard e gli eventi di "autorizzazione non riuscita" non vengono registrati nello stesso modo.

2.- Convalidare l'efficacia della mitigazione. Monitorare i registri di autenticazione dopo aver implementato l'autenticazione basata su certificati per verificare la riduzione degli eventi di autenticazione eccessivi. Il passaggio all'autenticazione basata su certificati ha consentito di ridurre gli attacchi e il rumore del registro.

Miglioramenti a lungo termine

Per risolvere i problemi sottostanti sono state create due richieste di funzionalità:

- Richiesta funzionalità 1: Aggiungere un'opzione per nascondere o visualizzare l'elenco dei gruppi di tunnel (profilo VPN) quando viene aggiunto un tenant VPN pubblico, riducendo l'individuabilità del profilo.
- Richiesta funzionalità 2: Aggiungere un'opzione di configurazione per abilitare o disabilitare la registrazione dei tentativi di autorizzazione VPN dell'Autorità registrazione non riusciti, consentendo agli amministratori di controllare il livello di dettaglio dei registri.

Inoltre, viene creato un documento pubblico per spiegare gli eventi registrati e il comportamento dell'autenticazione per aiutare gli amministratori a comprendere le normali operazioni di sistema.

Causa

La causa principale degli eventi di autenticazione eccessivi è la combinazione di profili VPN individuabili in configurazioni tenant pubbliche e il comportamento del flusso di autenticazione quando non è richiesta l'autenticazione basata su certificati. Quando l'autenticazione basata su RADIUS viene utilizzata senza requisiti di certificato, il sistema registra tutti i tentativi di "autorizzazione non riuscita" come parte della postura di sicurezza, compresi i tentativi da parte di attori esterni che individuano i profili VPN. Gli indirizzi locali del collegamento nei registri rappresentano il normale comportamento interno del sistema per il processo di autorizzazione dell'headend VPN dell'Autorità registrazione, non errori di configurazione.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

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).