

Funzione ISE RCM che provoca l'eliminazione dell'endpoint durante l'autenticazione basata su certificato

Sommario

Problema

Durante una migrazione da JAMF a MDM di Intune per i dispositivi macOS, Cisco ISE elimina o unisce in modo imprevisto i record degli endpoint e modifica le assegnazioni dei gruppi di identità degli endpoint durante l'autenticazione EAP-TLS.

Gli endpoint interessati vengono spostati dal gruppo di identità DB_Authorized_Devices a Profiled che attiva gli eventi CoA con il motivo "Eliminazione dell'endpoint". Ciò comporta la rimozione degli endpoint dal database interno ISE e l'interruzione dell'autenticazione per i dispositivi interessati. Il problema si verifica quando i dispositivi passano da una connessione wireless a una cablata e viceversa utilizzando lo stesso certificato contenente i campi URI della SAN (Subject Alternative Name) che ISE interpreta come GUID per la funzionalità Random and Changing MAC (RCM).

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.2
- endpoint macOS con autenticazione EAP-TLS
- Autenticazione basata su certificati con campi URI SAN contenenti identificatori di dispositivo
- Dispositivi che passano da una connessione di rete wireless a una di rete cablata e viceversa
- Migrazione MDM da JAMF a Microsoft Intune
- Funzione RCM (Random and Changing MAC) abilitata per impostazione predefinita in ISE 3.2

- Endpoint gestiti tramite API REST con attributi personalizzati

Risoluzione

Il problema è causato dalla funzionalità RCM di ISE 3.2, che unisce i record degli endpoint in base ai campi URI SAN del certificato. Sono disponibili due opzioni di risoluzione.

Opzione 1: Disattivare la funzionalità di RCM (scelta consigliata con attenzione)

Passaggio 1: Accesso all'interfaccia API ISE Swagger

Selezionare Amministrazione > Impostazioni > Impostazioni API e fare clic sul collegamento /swagger-ui.

Passaggio 2: Verifica impostazioni LSD correnti

Nell'interfaccia Swagger, individuare LSD Settings ed eseguire una richiesta GET per visualizzare la configurazione corrente:

```
GET /api/v1/lsd/settings
```

Passaggio 3: Modifica delle impostazioni di RCM

Eseguire una richiesta PUT con questo corpo per disabilitare RCM:

```
{  
  "enableEP0": true,  
}
```

```
"enableRCM": false  
}
```

Passaggio 4: Verifica della modifica della configurazione

Eseguire nuovamente la richiesta GET per verificare che RCM sia disabilitato e che LSD sia abilitato.

Passaggio 5: Esegui script di pulizia

Eseguire l'operazione di script consigliata per correggere le discrepanze tra gli attributi dopo la disabilitazione di RCM. Monitoraggio dell'infrastruttura per individuare eventuali corsie d'angolo durante il processo.



Attenzione: Possibile. I dettagli menzionati contengono procedure o comandi che potrebbero avere un impatto significativo se eseguiti. Assicurarsi che le procedure o i comandi siano stati valutati da uno SME o da una Business Unit prima di eseguire o consigliare.

Opzione 2: Modifica criteri di autorizzazione

Modificare i set di criteri per tenere conto del comportamento di RCM creando una logica di autorizzazione separata per i flussi di autenticazione cablati e wireless, garantendo che gli endpoint uniti ricevano decisioni di accesso appropriate in base al tipo di connessione anziché alla sola appartenenza ai gruppi di identità.

Elaborazione URI SAN certificato

ISE elabora i campi URI SAN dei certificati utilizzando una logica specifica per estrarre i GUID. Per i certificati contenenti segmenti Entra ID Microsoft, ISE rimuove i segmenti di identità transitori utilizzando il modello regex:

tag:[a-zA-Z0-9.,-]+:sid:S-[0-9-]+[: ,]?

Esempi di elaborazione URI SAN:

- Ingresso: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-133022741-66482"
- Archiviato nella sessione: "ID:Meraki:GUID:673288144292101809"

Causa

La funzionalità RCM (Random and Changing MAC) abilitata per impostazione predefinita in ISE 3.2 interpreta i campi degli URI SAN dei certificati come GUID per l'identificazione dell'endpoint. Quando i dispositivi che utilizzano lo stesso certificato si connettono tramite interfacce wireless e cablate, RCM unisce i record degli endpoint in base al GUID condiviso. Durante questo processo di unione, gli attributi dell'endpoint wireless vengono migrati nell'endpoint cablato e la voce MAC wireless viene eliminata dal database dell'endpoint. Questo comportamento si verifica prima che CoA o DHCP esegua i probe e comporta la perdita degli attributi personalizzati e delle assegnazioni dei gruppi di identità originariamente configurati tramite l'API REST. Il processo di unione non conserva gli attributi personalizzati che non fanno parte dei criteri di profilatura, con conseguente reimpostazione dell'identità dell'endpoint e successivi errori di autenticazione.

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).