

Función RCM de ISE que causa la eliminación de terminales durante la autenticación basada en certificados

Contenido

Problema

Durante una migración de JAMF a MDM de Intune para dispositivos macOS, Cisco ISE elimina o combina inesperadamente registros de terminales y cambia las asignaciones de grupos de identidad de terminales durante la autenticación EAP-TLS.

Los extremos afectados se mueven del grupo de identidad DB_Authorized_Devices al Profiel que desencadena eventos CoA con el motivo "Deleted of Endpoint". Como consecuencia, los terminales se eliminan de la base de datos interna de ISE y se producen interrupciones en la autenticación de los dispositivos afectados. El problema se produce cuando los dispositivos cambian entre conexiones inalámbricas y con cables utilizando el mismo certificado que contiene los campos URI de nombre alternativo del sujeto (SAN) que ISE interpreta como un GUID para la función de cambio aleatorio de MAC (RCM).

Entorno

- Cisco Identity Services Engine (ISE) versión 3.2
- terminales macOS con autenticación EAP-TLS
- Autenticación basada en certificados con campos URI de SAN que contienen identificadores de dispositivo
- Dispositivos que cambian entre conexiones de red por cable e inalámbricas
- Migración de MDM de JAMF a Microsoft Intune
- La función RCM (cambio aleatorio de MAC) está activada de forma predeterminada en ISE 3.2

- Terminales administrados mediante API REST con atributos personalizados

Resolución

El problema se debe a la función RCM de ISE 3.2, que combina registros de terminales basados en campos de certificado de URI de SAN. Hay dos opciones de resolución disponibles.

Opción 1: Desactivar la función del RCM (se recomienda con precaución)

Paso 1: Acceso a la interfaz API de ISE Swagger

Navegue hasta Administration > Settings > API Settings y haga clic en el enlace /swagger-ui.

Paso 2: Comprobar la configuración actual de LSD

En la interfaz de Swagger, busque LSD Settings y ejecute una solicitud GET para ver la configuración actual:

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

Paso 3: Modificar configuración del RCM

Ejecute una solicitud PUT con este cuerpo de solicitud para desactivar el RCM:

```
{  
  "enableEP0": true,  
  "enableRCM": false
```

}

Paso 4: Verificar el cambio de configuración

Ejecute de nuevo la solicitud GET para confirmar que el RCM está desactivado y que LSD permanece activado.

Paso 5: Ejecutar scripts de limpieza

Ejecute la operación de secuencia de comandos recomendada para corregir las discrepancias de atributos después de deshabilitar el RCM. Supervise la infraestructura en busca de casos de esquina durante este proceso.



Precaución: Posible. Los detalles mencionados aquí parecen contener procedimientos o comandos que podrían causar un impacto significativo si se ejecutan. Asegúrese de que los procedimientos o comandos han sido evaluados por una PYME o una unidad empresarial antes de ejecutarlos o recomendarlos.

Opción 2: Modificar directivas de autorización

Ajuste los conjuntos de políticas para tener en cuenta el comportamiento del RCM mediante la creación de una lógica de autorización independiente para los flujos de autenticación por cable e inalámbrica, lo que garantiza que los terminales combinados reciban las decisiones de acceso adecuadas en función del tipo de conexión, en lugar de únicamente en función de la pertenencia al grupo de identidad.

Procesamiento de URI de SAN de certificado

ISE procesa los campos de URI de SAN del certificado mediante una lógica específica para extraer los GUID. En el caso de certificados que contienen segmentos de Microsoft Entra ID, ISE

elimina los segmentos de identidad transitorios mediante el modelo de expresiones regulares:

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

Ejemplos de procesamiento SAN URI:

- Entrada: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Almacenado en la sesión: "ID:Meraki:GUID:673288144292101809"

Causa

La función RCM (Random and Changing MAC) activada de forma predeterminada en ISE 3.2 interpreta los campos de SAN URI de certificado como GUID para la identificación de terminales. Cuando los dispositivos que utilizan el mismo certificado se conectan a través de interfaces inalámbricas y con cables, el RCM combina los registros de terminales en función del GUID compartido. Durante este proceso de combinación, los atributos del terminal inalámbrico se migran al terminal con cables y la entrada MAC inalámbrica se elimina de la base de datos del terminal. Este comportamiento se produce antes de los sondeos de CoA o DHCP y da lugar a la pérdida de atributos personalizados y asignaciones de grupos de identidad que se configuraron originalmente a través de la API REST. El proceso de combinación no conserva los atributos personalizados que no forman parte de las directivas de generación de perfiles, lo que provoca el restablecimiento de la identidad del terminal y los consiguientes errores de autenticación.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).