

Recurso ISE RCM que causa exclusão de endpoint durante autenticação baseada em certificado

Contents

Problema

Durante uma migração do JAMF para o Intune MDM para dispositivos macOS, o Cisco ISE inesperadamente exclui ou mescla registros de ponto de extremidade e altera atribuições de grupo de identidade de ponto de extremidade durante a autenticação EAP-TLS.

Os pontos de extremidade afetados são movidos do grupo de identidade DB_Authorized_Devices para Profield, acionando eventos de CoA com o motivo "Exclusão de Ponto de Extremidade". Isso resulta na remoção de endpoints do banco de dados interno do ISE e causa interrupções de autenticação para os dispositivos afetados. O problema ocorre quando os dispositivos alternam entre conexões com e sem fio usando o mesmo certificado que contém os campos URI do Nome Alternativo da Entidade (SAN) que o ISE interpreta como um GUID para o recurso RCM (Random and Changing MAC).

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.2
- endpoints macOS que usam autenticação EAP-TLS
- Autenticação baseada em certificado com campos URI SAN contendo identificadores de dispositivo
- Dispositivos alternando entre conexões de rede com e sem fio
- Migração MDM de JAMF para o Microsoft Intune
- Recurso RCM (Random and Changing MAC) habilitado por padrão no ISE 3.2

- Endpoints gerenciados via API REST com atributos personalizados

Resolução

O problema é causado pelo recurso RCM no ISE 3.2, que mescla registros de endpoint com base nos campos de certificado do URI da SAN. Duas opções de resolução estão disponíveis.

Opção 1: Desabilitar Recurso RCM (Recomendado com Cuidado)

Passo 1: Acessar a interface de API do ISE Swagger

Navegue até Administration > Settings > API Settings e clique no link /swagger-ui.

Passo 2: Verificar Configurações Atuais de LSD

Na interface do Swagger, localize LSD Settings e execute uma solicitação GET para exibir a configuração atual:

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

Passo 3: Modificar Configurações do RCM

Execute uma solicitação PUT com este corpo de solicitação para desabilitar o RCM:

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

}

Passo 4: Verificar a alteração da configuração

Execute a solicitação GET novamente para confirmar se o RCM está desabilitado e o LSD permanece habilitado.

Passo 5: Executar Scripts de Limpeza

Execute a operação de script recomendada para corrigir discrepâncias de atributo após a desabilitação do RCM. Monitore a infraestrutura para todos os casos secundários durante esse processo.



Caution: Possível. Os detalhes mencionados aqui parecem conter procedimentos ou comandos que poderiam causar um impacto significativo se executados. Verifique se os procedimentos ou comandos foram avaliados por um SME ou Unidade de negócios antes de executar ou recomendar.

Opção 2: Modificar Políticas de Autorização

Ajuste os conjuntos de políticas para considerar o comportamento do RCM criando uma lógica de autorização separada para fluxos de autenticação com e sem fio, garantindo que os pontos finais mesclados recebam decisões de acesso apropriadas com base no tipo de conexão, em vez de somente na associação do grupo de identidade.

Processamento de URI SAN de Certificado

O ISE processa campos de URI de SAN de certificado usando lógica específica para extrair GUIDs. Para certificados contendo segmentos de ID do Microsoft Entra, o ISE retira segmentos de identidade transientes usando o padrão regex:

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

Exemplos de processamento de URI de SAN:

- Entrada: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Armazenado na sessão: "ID:Meraki:GUID:673288144292101809"

Causa

O recurso RCM (Random and Changing MAC) habilitado por padrão no ISE 3.2 interpreta os campos de certificado do URI da SAN como GUIDs para identificação do ponto de extremidade. Quando os dispositivos que usam o mesmo certificado se conectam por meio de interfaces com e sem fio, o RCM mescla os registros de endpoint com base no GUID compartilhado. Durante esse processo de mesclagem, os atributos do endpoint sem fio são migrados para o endpoint com fio, e a entrada MAC sem fio é excluída do banco de dados do endpoint. Esse comportamento ocorre antes das sondas CoA ou DHCP e resulta na perda de atributos personalizados e atribuições de grupos de identidade que foram originalmente configurados através da API REST. O processo de mesclagem não preserva atributos personalizados que não fazem parte das políticas de criação de perfil, levando à redefinição de identidade do ponto de extremidade e a falhas de autenticação subsequentes.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.