

ISE RCM-functie die eindpuntverwijdering veroorzaakt tijdens certificaatgebaseerde verificatie

Inhoud

uitgifte

Tijdens een migratie van JAMF naar Intune MDM voor macOS-apparaten verwijdert of voegt Cisco ISE onverwacht eindpuntrecords en wijzigt het de identiteitsgroep toe wijzingen van eindpunten tijdens EAP-TLS-verificatie.

De betreffende eindpunten worden verplaatst van de identiteitsgroep DB_Authorized_Devices naar Profiled waardoor CoA-gebeurtenissen worden geactiveerd met de reden "Deletion of Endpoint." Dit resulteert in het verwijderen van eindpunten uit de interne ISE-database en veroorzaakt uitval van de verificatie voor de getroffen apparaten. Het probleem treedt op wanneer apparaten switches tussen draadloze en bekabelde verbindingen met hetzelfde certificaatonderdeel dat de URI-velden voor alternatieve namen (SAN) bevat die ISE interpreteert als een GUID voor de functie Random and Changing MAC (RCM).

milieu

- Cisco Identity Services Engine (ISE) versie 3.2
- macOS-eindpunten met EAP-TLS-verificatie
- Certificaatgebaseerde verificatie met SAN URI-velden met apparaatid's
- Apparaten die schakelen tussen draadloze en bekabelde netwerkverbindingen
- MDM-migratie van JAMF naar Microsoft Intune
- RCM-functie (Random and Changing MAC) standaard ingeschakeld in ISE 3.2
- Eindpunten beheerd via REST API met aangepaste attributen

resolutie

Het probleem wordt veroorzaakt door de RCM-functie in ISE 3.2, die eindpuntrecords samenvoegt op basis van SAN URI-certificaatvelden. Er zijn twee resolutieopties beschikbaar.

Optie 1: RCM-functie uitschakelen (met de nodige voorzichtigheid aanbevolen)

Stap 1: Toegang tot de ISE Swagger API Interface

Navigeer naar Beheer > Instellingen > API-instellingen en klik op de link /swagger-ui.

Stap 2: Controleer de huidige LSD-instellingen

Zoek in de Swagger-interface naar LSD-instellingen en voer een GET-verzoek uit om de huidige configuratie te bekijken:

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

Stap 3: RCM-instellingen wijzigen

Voer een PUT-verzoek uit met dit aanvraagorgaan om RCM uit te schakelen:

```
{  
  "enableEPO": true,  
  "enableRCM": false  
}
```

Stap 4: Controleer de configuratiewijziging

Voer het GET-verzoek opnieuw uit om te bevestigen dat RCM is uitgeschakeld en LSD ingeschakeld blijft.

Stap 5: Schoonmaakscripts uitvoeren

Voer de aanbevolen scriptbewerking uit om verschillen in kenmerken op te lossen nadat RCM is uitgeschakeld. Houd de infrastructuur tijdens dit proces in de gaten voor eventuele hoekgevallen.



Let op: mogelijk. De hier genoemde details lijken procedures of opdrachten te bevatten die aanzienlijke gevolgen kunnen hebben als ze worden uitgevoerd. Zorg ervoor dat de procedures of opdrachten zijn geëvalueerd door een kmo of bedrijfseenheid voordat u ze uitvoert of aanbeveelt.

Optie 2: Wijzig het machtigingsbeleid

Beleidssets aanpassen om rekening te houden met RCM-gedrag door een afzonderlijke autorisatielogica voor bekabelde en draadloze verificatiestromen te maken, zodat samengevoegde eindpunten passende toegangsbeslissingen krijgen op basis van het verbindingstype in plaats van alleen het lidmaatschap van de identiteitsgroep.

SAN URI-verwerking van certificaten

ISE verwerkt SAN URI-velden voor certificaten met behulp van specifieke logica om GUID's te extraheren. Voor certificaten die Microsoft Entra ID-segmenten bevatten, stript ISE voorbijgaande identiteitssegmenten met behulp van het regex-patroon:

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

Voorbeelden van SAN URI-verwerking:

- Invoer: "ID: Meraki:GUID:673288144292101809:tag: microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Opgeslagen in sessie: "ID: Meraki: GUID: 673288144292101809"

Oorzaak

De RCM-functie (Random and Changing MAC) die standaard is ingeschakeld in ISE 3.2, interpreteert certificaatSAN URI-velden als GUID's voor eindpuntidentificatie. Wanneer apparaten met hetzelfde certificaat verbinding maken via zowel draadloze als bekabelde interfaces, voegt RCM de eindpuntrecords samen op basis van de gedeelde GUID. Tijdens dit samenvoegproces worden kenmerken van het draadloze eindpunt naar het bedrade eindpunt gemigreerd en wordt het draadloze MAC-item uit de endpoint-database verwijderd. Dit gedrag treedt op voordat CoA of DHCP sondes uitvoert en resulteert in het verlies van aangepaste attributen en identiteitsgroeptoewijzingen die oorspronkelijk waren geconfigureerd via REST API. Het samenvoegproces behoudt geen aangepaste kenmerken die geen deel uitmaken van het profielbeleid, wat leidt tot het opnieuw instellen van de eindpuntidentiteit en daaropvolgende verificatiefouten.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.