ISE RCM-Funktion verursacht Löschung von Endpunkten während der zertifikatbasierten Authentifizierung

Inhalt

Problem

Bei einer Migration von JAMF zu Intune MDM für MacOS-Geräte löscht oder führt die Cisco ISE während der EAP-TLS-Authentifizierung unerwartet Endpunktdatensätze und ändert die Zuweisung von Endpunkt-Identitätsgruppen.

Die betroffenen Endpunkte werden aus der Identitätsgruppe DB_Authorized_Devices in das Profil verschoben, das CoA-Ereignisse mit dem Grund "Deletion of Endpoint" auslöst. Dies führt dazu, dass Endpunkte aus der internen ISE-Datenbank entfernt werden, und verursacht Authentifizierungsausfälle für die betroffenen Geräte. Das Problem tritt auf, wenn Geräte zwischen drahtlosen und kabelgebundenen Verbindungen wechseln und dasselbe Zertifikat mit SAN-URI-Feldern (Subject Alternative Name) verwenden, das ISE als GUID für die RCM-Funktion (Random and Changing MAC) interpretiert.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.2
- MacOS-Endpunkte mit EAP-TLS-Authentifizierung
- Zertifikatsbasierte Authentifizierung mit SAN-URI-Feldern, die Geräteidentifikatoren enthalten
- Geräte, die zwischen drahtlosen und kabelgebundenen Netzwerkverbindungen wechseln
- MDM-Migration von JAMF zu Microsoft Intune
- RCM-Funktion (Random and Changing MAC) in ISE 3.2 standardmäßig aktiviert

- Über REST-API verwaltete Endgeräte mit benutzerdefinierten Attributen

Auflösung

Das Problem wird durch die RCM-Funktion in ISE 3.2 verursacht, bei der Endpunktdatensätze auf Basis der SAN-URI-Zertifikatfelder zusammengeführt werden. Es stehen zwei Auflösungsoptionen zur Verfügung.

Option 1: Deaktivieren der RCM-Funktion (mit Vorsicht empfohlen)

Schritt 1: Zugriff auf die ISE Swagger API-Schnittstelle

Navigieren Sie zu Administration > Settings > API Settings, und klicken Sie auf den Link /swagger-ui.

Phase 2: Aktuelle LSD-Einstellungen überprüfen

Suchen Sie in der Swagger-Schnittstelle nach den LSD-Einstellungen, und führen Sie eine GET-Anforderung aus, um die aktuelle Konfiguration anzuzeigen:

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

Schritt 3: RCM Einstellungen ändern

Führen Sie eine PUT-Anforderung mit diesem Anforderungstext aus, um den RCM zu deaktivieren:

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

Schritt 4: Überprüfen der Konfigurationsänderung

Führen Sie die GET-Anforderung erneut aus, um zu bestätigen, dass der RCM deaktiviert ist und LSD aktiviert bleibt.

Schritt 5: Cleanup-Skripts ausführen

Führen Sie den empfohlenen Skriptvorgang aus, um Attributabweichungen nach der RCM-Deaktivierung zu beheben. Überwachen Sie die Infrastruktur während dieses Prozesses auf alle Eckfälle.

⚠ Vorsicht: Möglich. Die hier genannten Details enthalten offenbar Prozeduren oder Befehle, die bei ihrer Ausführung erhebliche Auswirkungen haben könnten. Stellen Sie sicher, dass die Verfahren oder Befehle von einem SME oder einem Geschäftsbereich evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Option 2: Autorisierungsrichtlinien ändern

Anpassen von Richtliniensätzen zur Berücksichtigung des RCM-Verhaltens durch Erstellen einer separaten Autorisierungslogik für kabelgebundene und Wireless-Authentifizierungsflüsse, um sicherzustellen, dass zusammengeführte Endgeräte geeignete Zugriffsentscheidungen erhalten, die auf dem Verbindungstyp und nicht nur auf der Identitätsgruppenmitgliedschaft basieren.

Zertifikat-SAN-URI-Verarbeitung

ISE verarbeitet SAN-URI-Zertifikatfelder mithilfe einer bestimmten Logik, um GUIDs zu

extrahieren. Bei Zertifikaten, die Microsoft Entra ID-Segmente enthalten, entfernt die ISE vorübergehende Identitätssegmente unter Verwendung des Regex-Musters:

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

Beispiele für die SAN URI-Verarbeitung:

- Eingabe: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Gespeicherte Sitzung: "ID:Meraki:GUID:673288144292101809"

Ursache

Die in ISE 3.2 standardmäßig aktivierte RCM-Funktion (Random and Changing MAC) interpretiert SAN-URI-Zertifikatfelder als GUIDs für die Endpunktidentifizierung. Wenn Geräte, die dasselbe Zertifikat verwenden, über Wireless- und kabelgebundene Schnittstellen eine Verbindung herstellen, führt der RCM die Endpunktdatensätze basierend auf der gemeinsam genutzten GUID zusammen. Bei diesem Zusammenführungsprozess werden Attribute vom Wireless-Endpunkt zum kabelgebundenen Endpunkt migriert, und der Wireless-MAC-Eintrag wird aus der Endpunktdatenbank gelöscht. Dieses Verhalten tritt vor CoA- oder DHCP-Tests auf und führt zum Verlust benutzerdefinierter Attribute und Identitätsgruppenzuweisungen, die ursprünglich über die REST-API konfiguriert wurden. Beim Mergeprozess werden benutzerdefinierte Attribute, die nicht Teil der Profilerstellungsrichtlinien sind, nicht beibehalten. Dies führt zum Zurücksetzen der Endpunktidentität und anschließenden Authentifizierungsfehlern.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.