Fehlerbehebung bei ISE Agentenloser Status nach Sitzungsneuauthentifizierung wird nicht ausgelöst

Inhalt

Problem

Die agentenlose Statusfunktion in der Identity Services Engine (ISE) 3.3 kann nach den Ereignissen zur Sitzungsneuauthentifizierung nicht ausgelöst werden. Während der Erstauthentifizierung funktioniert der agentenlose Status ordnungsgemäß, und die Endpunkte werden kompatibel. Bei einer erneuten Authentifizierung erhalten Endpunkte jedoch RADIUS Accounting Interim Update-Ereignisse anstelle von Accounting Start-Ereignissen, sodass der agentenlose Statusfluss nicht aufgerufen wird. Daher stimmen die Endgeräte mit einer unbekannten Statusrichtlinie überein und verbleiben in einem unbekannten Status, was sich auf den Netzwerkzugriff für die betroffenen Geräte auswirkt.

Das Problem tritt bei Endpunkten auf, die nach der erneuten Authentifizierung den Status "Status ausstehend" oder "Unbekannt" erhalten haben, wobei ca. 800 von 1.200 Endpunkten in der berichteten Umgebung betroffen sind. Die Protokollanalyse zeigt, dass die ISE bei der erneuten Authentifizierung ACCOUNTING_UPDATE-Ereignisse mit agentlessEnabled=true empfängt, der Statusfluss jedoch für die vorhandene Sitzungs-ID nicht erneut aufgerufen wird.

Umwelt

- Identity Services Engine (ISE) Version 3.3 Patch 4
- Kabelgebundene 802.1X-Authentifizierung mit MAC Authentication Bypass (MAB)
- Agentenlose Statuskonfiguration aktiviert
- Konfigurierte Timer für die erneute Authentifizierung der Sitzung (Zeitüberschreitung von 420 Sekunden)
- Cisco Catalyst Switches als Netzwerkzugriffsgeräte
- Etwa 1.200 Endpunkte in der Umgebung

Auflösung

Dieses Verhalten wird von der ISE erwartet und ist vom Design her möglich. Agentenloser Status wird nur durch RADIUS Accounting-Startereignisse ausgelöst und darf nicht durch Accounting-Zwischenaktualisierungsereignisse während der erneuten Authentifizierung von Sitzungen erneut aufgerufen werden, wenn die Framed IP-Adresse unverändert bleibt.

Technische Analyse

Der ISE NetAccessEventHandler-Codepfad führt nur eine Neuarmierung des agentenlosen Statusflusses für frische RADIUS Accounting-Start-Pakete durch. Während der erneuten Authentifizierung senden Netzwerkgeräte in der Regel Accounting Interim-Update-Pakete mit derselben Acct-Session-Id, wodurch die Funktion shouldInvokePostureFlow() false zurückgibt, wodurch eine Statusneubewertung verhindert wird.

Protokollnachweis, der das Verhalten anzeigt:

Anfängliche Authentifizierung (Agentenloser Status wird ausgelöst):

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Neuauthentifizierung (Agentenloser Status nicht ausgelöst):

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Empfohlene Lösung

Um die Auswirkungen dieses Verhaltens zu mindern, konfigurieren Sie Lease-Einstellungen für den Status, um die Endpunkt-Compliance während der Neuauthentifizierung aufrechtzuerhalten:

Schritt 1: Konfigurieren Sie in ISE-Statusrichtlinien die entsprechende Leasingdauer, um sicherzustellen, dass die Endpunkte zwischen den Statusüberprüfungen keinen Netzwerkzugriff verlieren.

Phase 2: Überwachen Sie den Endgerätestatus und passen Sie die Lease-Timer an, je nach den Sicherheitsanforderungen Ihres Unternehmens und der Häufigkeit der erneuten Authentifizierung.

Ursache

Dies ist ein erwartetes Verhalten, das in Cisco Bug-ID CSCwu48086 dokumentiert ist. Der Agentenlose Status in ISE ist nur für die Auslösung von RADIUS Accounting-Startereignissen konzipiert und wird nicht durch Interim Accounting-Aktualisierungsereignisse ausgelöst. Während der Neuauthentifizierung von Sitzungen senden Netzwerkzugriffsgeräte Accounting Interim Updates mit derselben Frame-IP-Adresse und Session-ID, die den agentenlosen Statusüberprüfungsprozess nicht erneut aufrufen. Der ISE-Code überprüft insbesondere, ob neue Sitzungen (ACCOUNTING_START-Ereignisse) vorhanden sind, bevor er agentenlose Statusdatenflüsse initiiert.

Verwandte Inhalte

- Cisco Bug-ID CSCwu48086
- 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.