Problemen oplossen ISE Agentless-houding wordt niet geactiveerd na sessieherverificatie

Inhoud

uitgifte

Agentless posture-functionaliteit in Identity Services Engine (ISE) 3.3 kan niet worden geactiveerd na gebeurtenissen voor sessieherverificatie. Tijdens de eerste verificatie werkt de agentloze houding correct en worden eindpunten compliant. Wanneer echter opnieuw wordt geverifieerd, ontvangen eindpunten de RADIUS Accounting Interim Update-gebeurtenissen in plaats van de gebeurtenissen voor het starten van de boekhouding, waardoor de agentloze posturele stroom niet wordt aangeroepen. Als gevolg hiervan komen eindpunten overeen met een onbekend houdingsbeleid en blijven ze in een onbekende houdingsstaat, wat van invloed is op de netwerktoegang voor getroffen apparaten.

Het probleem manifesteert zich met eindpunten die vastzitten in de status "Posture Pending" of "Unknown" na herverificatie, waarbij ongeveer 800 van de 1200 eindpunten zijn aangetast in de gerapporteerde omgeving. Uit loganalyse blijkt dat ISE tijdens de herverificatie ACCOUNTING_UPDATE-gebeurtenissen ontvangt met agentlessEnabled=true, maar dat de posturele stroom niet opnieuw wordt aangeroepen voor de bestaande sessie-ID.

milieu

- Identity Services Engine (ISE) versie 3.3 Patch 4
- Bekabelde 802.1X-verificatie met MAC-verificatiebypass (MAB)
- Configuratie van positie zonder agents ingeschakeld
- Tijdsduur voor herverificatie van sessie geconfigureerd (time-out van 420 seconden)
- Cisco Catalyst-switches als netwerktoegangsapparaten
- Ongeveer 1200 eindpunten in het milieu

resolutie

Dit gedrag wordt verwacht en door ontwerp in ISE. De positie van de agent wordt alleen geactiveerd door de gebeurtenissen bij de start van de boekhouding van RADIUS en mag niet opnieuw worden aangeroepen door de gebeurtenissen bij de tussentijdse boekhoudkundige update tijdens de herverificatie van de sessie wanneer het IP-adres van het frame ongewijzigd blijft.

technische analyse

Het ISE NetAccessEventHandler-codepad bewapent alleen de agentloze posturele stroom op nieuwe RADIUS Accounting-Start-pakketten. Tijdens de herverificatie verzenden netwerkapparaten doorgaans pakketten met dezelfde Act-Session-ID, waardoor de functie shouldInvokePostureFlow() false teruggeeft, waardoor een herevaluatie van de houding wordt voorkomen.

Logbewijs dat het gedrag toont:

Initiële verificatie (Agentless Posture Trigged):

```
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
```

Reauthenticatie (Agentless-houding niet geactiveerd):

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

Aanbevolen workaround

Om de impact van dit gedrag te beperken, configureert u de houdingsleaseinstellingen om de naleving van het eindpunt tijdens herverificatiescenario's te handhaven:

Stap 1: Configureer de juiste leaseduur voor de houding in het ISE-houdingsbeleid om ervoor te zorgen dat eindpunten geen netwerktoegang verliezen tussen houdingsevaluaties.

Stap 2: Bewaak de eindpuntstatus en pas leasetimers aan op basis van de beveiligingsvereisten en herverificatiefrequentie van uw organisatie.

Oorzaak

Dit wordt verwacht gedrag gedocumenteerd in Cisco Bug ID CSCwu48086. De agentloze houding in ISE is zodanig ontworpen dat deze alleen wordt geactiveerd bij gebeurtenissen in de RADIUS Accounting Start en wordt niet geactiveerd door tussentijdse boekhoudkundige update. Tijdens sessieherverificatie verzenden netwerktoegangsapparaten tussentijdse boekhoudupdates met hetzelfde IP-adres en sessie-ID in Framed, die het beoordelingsproces van de lichaamshouding zonder agents niet opnieuw oproepen. De ISE-code controleert specifiek op nieuwe sessies (ACCOUNTING_START-gebeurtenissen) voordat de agentloze houdingsstromen worden gestart.

Gerelateerde inhoud

- Cisco Bug ID CSCwu48086
- 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.