Upgrade van snort-engine geblokkeerd tijdens FTD-upgrade vanwege aangepaste beleidsdetectie

Inhoud

uitgeven

Tijdens een FTD-upgrade van versie 7.2 naar 7.4.4 op een door FMC beheerde HA FPR-4115 wordt de Snort-engine-upgrade naar Snort 3 geblokkeerd met foutmeldingen die aangeven dat de aangepaste regels van Snort 2 niet zijn omgezet of dat aangepaste inbraak- of netwerkanalysebeleid is gebruikt. De specifieke foutmelding vermeldt: "Kan niet upgraden naar Snort 3. Apparaat gebruikt ten minste één aangepast inbraakbeleid of netwerkanalysebeleid." Een meer gedetailleerde foutmelding verwijst naar het onvermogen om aangepaste Snort 2-regels te converteren en verwijst naar /var/sf/htdocs/ips/snort.rej voor meer informatie. De vraag is of deze fout migratie naar Snort 3 en de inspectiefunctionaliteit zou voorkomen.

milieu

- Cisco Secure Firewall Firepower versie 7.3
- Firepower Management Center (FMC) versie 7.7.11
- FTD-apparaten in High Availability (HA)-configuratie
- Hardware: FPR-4115
- Upgradepad: FTD 7.2 tot 7.4.4
- VDB ten laatste versie vóór upgrade
- Lokale regels sectie onder Objecten > Inbraakregels > Snort 2 Alle regels is leeg

resolutie

De foutmelding die de Snort-engine-upgrade blokkeert, is gedocumenteerd gedrag met betrekking tot Cisco-bug-ID CSCwn46794 en vertegenwoordigt geen functionele blokkering wanneer er geen werkelijke aangepaste Snort 2-regels bestaan.

Verificatiestappen

Stap 1: Status aangepaste snort 2-regels controleren

Navigeer naar de FMC-interface en controleer of er aangepaste Snort 2-regels zijn:

```
Objecten > Inbraakregels > Alle regels 2 snuiven > Lokale regels
```

Stap 2: VDB-versie bevestigen

Zorg ervoor dat de kwetsbaarheidsdatabase (VDB) de laatste versie is voordat u doorgaat met de upgrade.

Stap 3: Foutdetails bekijken

Controleer de gedetailleerde foutinformatie in het bestand waarnaar wordt verwezen:

```
/var/sf/htdocs/ips/snort.rej
```

Upgradeproces

Wanneer de sectie "Lokale regels" leeg blijkt te zijn (er zijn geen aangepaste Snort 2-regels aanwezig), kan de upgrade doorgaan ondanks de foutmelding. De blokkeringsfout is een fout-positief in dit scenario en geeft geen werkelijke aangepaste regels aan die moeten worden geconverteerd.

Stap 1: doorgaan met Snort 3-upgrade

Ga verder met het FTD-upgradeproces naar versie 7.4.4, inclusief de Snort 3-motorupgrade.

Stap 2: Validatie na upgrade

Nadat de upgrade met succes is voltooid, test u de verkeersstroom om het verwachte gedrag met de Snort 3-motor te bevestigen.

Stap 3: Bewaken van de systeemprestaties

Valideer dat de inspectiefunctionaliteit werkt zoals verwacht met de nieuwe Snort 3-motor.

Oorzaak

Het blokkeringsbericht voor de upgrade is gedocumenteerd gedrag dat is gekoppeld aan Cisco-bug-ID CSCwn46794. Deze bug zorgt ervoor dat het systeem een foutmelding weergeeft over aangepast inbraakbeleid of netwerkanalysebeleid, zelfs als er geen aangepaste Snort 2-regels bestaan die conversie vereisen. De foutmelding wordt weergegeven als een fout-positief wanneer de sectie Lokale regels leeg is, maar de validatie van het systeem voorafgaand aan de upgrade identificeert ten onrechte de aanwezigheid van aangepaste beleidsregels.

Verwante inhoud

- Cisco bug ID CSCwn46794
- Cisco bug ID CSCwk07199
- 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.