Secure Firewall FTD Password Reset na wachtwoordverlies

uitgeven

Firewall Threat Defense (FTD) werd ontoegankelijk via CLI vanwege een verloren lokaal beheerderswachtwoord. Het getroffen knooppunt kon niet worden geopend voor administratieve doeleinden. De aanvankelijke veronderstelling was dat het beheerderswachtwoord was gewijzigd ten opzichte van de standaardwaarde en onbekend was, wat leidde tot bezorgdheid dat een volledige fabrieksreset (opnieuw instellen van image) nodig zou zijn om toegangs- en standaardreferenties te herstellen. Er zijn specifieke vragen gerezen over de juiste procedure voor het omgaan met deze situatie:

milieu

- Cisco Secure Firewall 1000, 2100 en 3100 FTD beheerd Firepower Management Center

resolutie

De resolutie betrof het proberen toegang te krijgen tot het getroffen FTD-apparaat met behulp van de standaard beheerdersreferenties voordat de meer complexe procedure voor het opnieuw installeren van images werd voortgezet.

1: Probeer voordat u begint in te loggen op het betreffende FTD-apparaat met behulp van de standaard beheerdersreferenties van de fabriek.

```
Username: admin
Password: Admin123
```

Deze stap moet eerst worden uitgevoerd, omdat hierdoor de noodzaak van meer verstorende

herstelprocedures kan worden geëlimineerd.

2: Als standaardreferenties zijn uitgesloten, stelt u het beheerderswachtwoord opnieuw in op een nieuwe, bekende waarde via de standaard FTD CLI-procedure voor het wijzigen van het wachtwoord.

Installatiekopie installeren: Cisco Secure Firewall ASA en Handleiding voor installatiekopie voor bedreigingsbeveiliging

- Voer een volledige reimage uit van het betreffende FTD-apparaat, volgens de stappen in de Cisco-documentatie.
- Standaardreferenties in de fabriek herstellen via het proces voor het opnieuw installeren van images.

Oorzaak

De hoofdoorzaak was dat het beheerderswachtwoord op het betreffende FTD-apparaat tijdens de eerste implementatie nooit was gewijzigd ten opzichte van de fabrieksinstellingen. Het verlies van toegang was te wijten aan de onjuiste veronderstelling dat het wachtwoord onbekend was, in plaats van een daadwerkelijk verlies van referenties. Het apparaat bleef gedurende het hele incident toegankelijk met behulp van de standaard beheerdersreferenties.

Verwante inhoud

- Vervang defecte eenheid in beveiligde firewall-dreiging Verweer van hoge beschikbaarheid
- Cisco FXOS-handleiding voor probleemoplossing voor de bescherming tegen firewallbedreigingen: imagebeheer
- Cisco Secure Firewall ASA en Threat Defense Reimage Guide
- Configureren, verifiëren en problemen oplossen bij registratie van Firepower-apparaten
- Hoge beschikbaarheid van FTD op Firepower-applicaties configureren
- 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.