FTD-Kennwort der sicheren Firewall zurücksetzen nach Kennwortverlust

Problem

Der Zugriff auf die Firewall-Bedrohungsabwehr (FTD) über die CLI wurde aufgrund eines verlorenen lokalen Administratorkennworts unmöglich. Auf den betroffenen Knoten konnte nicht aus administrativen Gründen zugegriffen werden. Ursprünglich wurde davon ausgegangen, dass das Admin-Kennwort vom Standard abgeändert wurde und unbekannt ist. Dies gab Anlass zu der Sorge, dass ein vollständiges Zurücksetzen (erneutes Abbild) erforderlich ist, um den Zugriff und die Standardanmeldeinformationen wiederherzustellen. Spezielle Fragen betrafen das richtige Verfahren für die Behandlung dieser Situation:

Umwelt

- Cisco Secure Firewall 1000, 2100 und 3100 FTD Managed FirePOWER Management Center

Auflösung

Die Lösung beinhaltete den Versuch, mit den standardmäßigen Admin-Anmeldedaten auf das betroffene FTD-Gerät zuzugreifen, bevor mit dem komplexeren Verfahren zum erneuten Abbild fortgefahren wird.

1: Bevor Sie beginnen, versuchen Sie, sich mit den werkseitigen Standardanmeldeinformationen für den Administrator beim betroffenen FTD-Gerät anzumelden.

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

Dieser Schritt muss zuerst durchgeführt werden, da sonst störendere Wiederherstellungsverfahren erforderlich wären.

2: Wenn Standardanmeldeinformationen ausgeschlossen sind, setzen Sie das Admin-Kennwort mithilfe des Standardverfahrens zur Änderung des FTD-CLI-Kennworts auf einen neuen, bekannten Wert zurück.

Neubildprozess: Cisco Secure Firewall ASA und Threat Defence - Image-Leitfaden

- Führen Sie ein vollständiges Rebimage des betroffenen FTD-Geräts unter Beachtung der Schritte in der Cisco Dokumentation durch.
- Stellen Sie die werkseitigen Standardanmeldeinformationen mithilfe des Neuabbildungsprozesses wieder her.

Ursache

Die Ursache dafür war, dass das Administratorkennwort auf dem betroffenen FTD-Gerät bei der Erstbereitstellung nie gegenüber der werkseitigen Standardeinstellung geändert wurde. Der Verlust des Zugriffs war auf die falsche Annahme zurückzuführen, dass das Kennwort unbekannt war, und nicht auf einen tatsächlichen Verlust der Anmeldeinformationen. Der Zugriff auf das Gerät blieb während des Vorfalls mit den Standardanmeldeinformationen für Administratoren möglich.

Verwandte Inhalte

- Austausch defekter Einheiten bei hochverfügbarer Abwehr von Bedrohungen durch sichere Firewall
- Cisco FXOS-Fehlerbehebungshandbuch für die Firewall-Bedrohungsabwehr: Image-Management
- Cisco Secure Firewall ASA und Threat Defence - Image-Leitfaden
- Konfiguration, Überprüfung und Fehlerbehebung bei der Registrierung von FirePOWER-Geräten
- Konfigurieren von FTD-Hochverfügbarkeit auf Firepower-Appliances
- 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.