セキュアファイアウォールFTDパスワードリセット ；パスワード喪失後

お問い合わせ内容

ローカル管理者パスワードが失われたため、ファイアウォール脅威対策(FTD)にCLI経由でアクセスできなくなりました。管理の目的で該当ノードにアクセスできませんでした。当初の想定では、管理者パスワードがデフォルトから変更されて不明であったため、アクセスとデフォルトのクレデンシャルを復元するために完全な工場出荷時設定へのリセット（再イメージ化）が必要になることが懸念されていました。この状況を処理するための適切な手順に関して、特定の質問が発生しました。

環境

- Cisco Secure Firewall 1000、2100、および3100 FTDマネージドFirepower Management Center

解決策

この問題を解決するには、より複雑な再イメージ化手順に進む前に、デフォルトの管理者クレデンシャルを使用して該当のFTDデバイスにアクセスする必要がありました。

1：最初に、工場出荷時のデフォルトの管理者クレデンシャルを使用して、該当するFTDデバイスにログインしてみます。

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

このステップを最初に実行してください。このステップを実行すると、より中断を伴うリカバリ手順が不要になります。

2：デフォルトのクレデンシャルが除外された場合は、標準のFTD CLIパスワード変更手順で、管理者パスワードを新しい既知の値にリセットします。

再イメージ化プロセス：Cisco Secure Firewall ASAおよび脅威対策の再イメージングガイド

- シスコの文書の手順に従って、該当するFTDデバイスの完全な再イメージ化を実行します。
- 再イメージ化プロセスを通じて、工場出荷時のデフォルトのクレデンシャルを復元します。

原因

根本原因は、初期導入時に、該当するFTDデバイスの管理者パスワードが工場出荷時のデフォルトから変更されていないことにあります。このアクセス不能は、実際にクレデンシャルが失われるのではなく、パスワードが不明であるという誤った仮定が原因でした。デバイスは、インシデントの間、デフォルトの管理者クレデンシャルを使用してアクセス可能なままです。

関連コンテンツ

- ハイアベイラビリティのセキュアファイアウォール脅威対策における障害ユニットの交換
- ファイアウォールの脅威対策に関するCisco FXOSトラブルシューティングガイド：イメージ管理
- Cisco Secure Firewall ASAおよび脅威対策の再イメージングガイド
- Firepowerデバイス登録の設定、確認、トラブルシューティング
- Firepower アプライアンスでの FTD 高可用性の設定
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。