

ISE管理GUIのログインがPingIDフェデレーションRADIUSトークンで失敗する

内容

問題

Ping FederateがAccess-Accept応答を返すことを示すパケットキャプチャにもかかわらず、PingIDフェデレーションをRADIUSトークンとして使用すると、Cisco ISEへの管理者GUIログインが失敗します。RADIUS認証がネットワークの観点からは成功しているように見えても、ログインが失敗し、ISEインターフェイスへの管理アクセスができなくなります。ネットワークパケット分析により、PingIDサーバ(10.32.154.200)が予期されるAccess-Accept応答(10.2.200.241)をISEに送信するものの、ISE管理ログインプロセスが正常に完了しないことが確認されます。

環境

- Cisco Identity Services Engine(ISE)バージョン3.3パッチ7
- 4ノードVM導入
- RADIUSトークン認証として構成されたpingIDフェデレーション
- ISE IPアドレス : 10.2.200.241
- PingIDサーバのIPアドレス : 10.32.154.200
- Admin Accessの設定をAdministration > Admin Accessで確認

解決方法

この問題は、管理者ログイン機能を正常にイネーブルにする回避策を適用することで解決されました。次のセクションで説明する手順は、この問題を解決するために実行されたものです。

ステップ1：証拠の収集と分析

パケットキャプチャの証拠が収集および分析され、ISEとPingIDサーバ間のRADIUS認証フローが確認されました。分析により、Ping FederateがAccess-Accept応答を正しく送信していることが確認されました。

ステップ2: prrt-server.logの証拠

###

prrt-server.logファイル

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

ステップ3：メッセージ認証者とは何ですか。

Message-Authenticator (Mオーセンティケーター) は、ネットワークデバイスとRADIUSサーバの
間で交換されるメッセージの整合性と信頼性を保証するためにRADIUSパケットで使用されるセ
キュリティ属性です。これは、共有秘密キーを使用してRADIUSパケット全体でHMAC-MD5を使
用して計算される暗号署名です。この属性は、特にExtensible Authentication Protocol(EAP)認証
フローに関連するRADIUSメッセージの改ざんやスプーフィングからの保護に役立ちます。

ステップ4：回避策の実装

「Message Authenticator Required On Response」を無効にします (管理/アイデンティティ管理
/外部アイデンティティソース/RADIUSトークン)。RADIUSトークン名をクリックし、
Authenticationに移動します。「Message Authenticator Required On Response」のチェックを外

します。

ステップ5：検証テスト

回避策を適用した後、admin loginテストを実行して解決策を検証しました。これらのテストにより、認証が成功し、RADIUSトークンとしてPingIDフェデレーションを使用してISE管理GUIにアクセスできることが確認されました。

ステップ6：モニタリング期間

回避策の安定性を確保するため、監視と検証の期間を設けました。この期間中、エラーや障害が報告されることなく、管理者ログインテストが継続的に実施されました。

原因

ISE管理GUIのログイン失敗は、MFA認証中のCisco ISE 3.3パッチ7とPingID(Ping Federate)間でのRADIUSプロトコルセキュリティ適用の不一致が原因で発生しました。

具体的には、

- Cisco ISE では、外部RADIUSトークンサーバからのAccess-Accept応答内に存在するRADIUS Message-Authenticator属性が必要です。
- PingIDがMessage-Authenticator属性なしでAccess-Accept応答を返していました。
- ISEでは設定Message Authenticator Required On Response が有効になっているので、PingID側で認証自体が成功した場合でも、RADIUS応答が無効であるとしてサイレントに拒否されました。
- この適用は、Blast-RADIUSの脆弱性(CVE-2024-3596)を軽減するためのCisco ISEのセキュリティ強化の一部です。

関連コンテンツ

- [Blast-RADIUSプロトコルスプーフィングの軽減\(CVE-2024-3596\)](#)

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。