Field Notice:FN70610:Android 10、Android 11、およびApple iOS 14デバイスでモバイルクライアントデバイスのMACランダム化が原因で、Cisco Identity Services Engine(ISE)のMACアドレスのルックアップが失敗する可能性 – 回避策を提供

通知

この Field Notice は現状のままで提供され、市場性の保証を含むいっさいの保証、あるいはサービス保証を示唆するものではありません。この Field Notice での情報、あるいは、この Field Notice からのリンク先資料はお客様ご自身の責任においてご使用をお願いいたします。シスコでは、任意の時点でこの Field Notice を変更あるいはアップデートする権利を留保いたします。

改訂履歴

改訂	発行日	注釈
1.0	2020年9月15日	初版リリース
1.1	2020年9月16日	「回避策/解決方法」セクションを更新
1.2	2020年9月18日	「影響を受ける製品」セクションを更新
1.3	2020年9月23日	問題の説明、背景、問題の症状、追加情報のセクションを更新。

影響を受ける製品

影響を受ける OS タイプ	影響を受けるソフトウェア製品	影響を受けるリリース	影響を受けるリリース番号	注釈
IOS 以外	Identity Services Engine システム ソフトウェア	1	1.0、1.0 MR、1.1、1.1.1、1.1.2、1.1.3、1.1.4、1.2、1.2.1、1.3、1.4	ISEのすべてのバージョンが影響を受けます
IOS 以外	Identity Services Engine システム ソフトウェア	2	2.0、2.0.1、2.1.0、2.2.0、2.2.1、2.3.0、2.4.0、2.6.0、2.7.0	ISEのすべてのバージョンが影響を受けます

IOS 以外	Identity Services Engine システム ソフトウェア	3	3.0.0	ISEのすべてのバージョンが影響を受けます

不具合情報

不具合 ID	見出し
CSCvv71694	IOS 14およびAndroid 10のMacランダム化により、BYOD、プロファイラ、およびMDMのフローが中断される可能性がある

問題の説明

Android 10、Android 11、およびApple iOS 14デバイスでは、モバイルクライアントデバイスでMACアドレスのランダム化が使用されるため、MACアドレスのルックアップを使用するCisco Identity Services Engine(ISE)サービスが失敗し、これらのデバイスで予期しないネットワーク接続の中断が発生する可能性があります。

背景

Android 10、Android 11、およびApple iOS 14デバイスは、ワイヤレスネットワークへの接続時にランダム化されたMACアドレスを使用して、ユーザにプライバシーを提供します。ISEおよび多くのネットワークコンポーネントでは、MACアドレスは特定のエンドポイントの一意のIDと見なされます。MACアドレスのランダム化により、この1対1のマッピングは正しくなくなり、1つのエンドポイントがISEデータベース(DB)内で複数のエンドポイントエントリを生成する可能性があります。

次の項では、MACアドレスのランダム化がモバイルエンドポイントでどのように実装されるかを示します。

Google Android 10およびAndroid 11

- ランダム化はデフォルトで有効になっています。
- ユーザが以前のバージョンのAndroidからAndroid 10またはAndroid 11にアップグレードした場合、保存されたサービスセット識別子(SSID)はランダム化されずに設定されたままになります。
- ランダム化は、ネットワークプロファイル(SSID)ごとに設定できます。
- 任意のネットワークプロファイルにランダムなMACアドレスが使用されると、ユーザがネットワークプロファイルを削除してSSID/ネットワークプロファイルを再作成した後でも、モバイルデバイスは同じランダムなMACアドレスを使用し続けます。
- Android MACランダム化の詳細については、「プライバシー： MACランダム化」を参照してください。

Apple iOS 14、iPad OS 14、およびwatchOS 7

- ランダム化はデフォルトで有効になっています。
- ユーザが以前のバージョンのiOSからiOS 14にアップグレードすると、既存のすべてのSSIDに対してランダム化が有効になります。
- ランダム化は、ネットワークプロファイル(SSID)ごとに設定できます。
- 任意のネットワークプロファイルにランダムなMACアドレスが使用されると、ユーザがネットワークプロファイルを削除してSSID/ネットワークプロファイルを再作成した後でも、モバイルデバイスは同じランダムなMACアドレスを使用し続けます。
- iOS MACランダム化の詳細については、「iOS 14、iPadOS 14、およびwatchOS 7でプライベートWi-Fiアドレスを使用する」を参照してください。

問題の症状

MACアドレスのランダム化のポリシーを準備しないと、新しいMACアドレスのランダム化動作が有効になった後で、以前にプロビジョニングされたモバイルデバイスとプロファイリングIDグループに基づいて設定されたポリシーが正しく一致しない可能性があります。その結果、これらのモバイルデバイスのネットワーク接続が切断される可能性があります。

MACアドレスのランダム化は、特定のデバイスの単一MACアドレスのマッピングに依存する次のISEサービスに影響します。

- 個人所有デバイスの持ち込み(BYOD):BYODオンボーディング時のクライアントのMACアドレスが、クライアントに返される証明書に組み込まれます。このため、オンボーディングSSIDとセキュアSSIDの間のMACアドレスが異なるため、MAC-in-SANまたはBYOD_is_Registered状態を使用するデュアルSSIDフローは失敗します。以前のバージョンのApple iOSからiOS 14にアップグレードされたデバイスのシングルSSIDフロー（Android 10またはAndroid 11にアップグレードされたデバイスのシングルSSIDフローは影響を受けません）の場合も、デバイス上のすべてのSSIDでMACアドレスのランダム化がデフォルトで有効になるため、この問題が発生します。
- プロファイリング：特定のプロファイリングポリシーは、一致しなくなったベンダーの組織固有識別子(OUI)に依存します。ランダム化されたMACアドレスは、特定のベンダーに固有ではないOUIのカスタム範囲を利用します。
- モバイルデバイス管理(MDM):ISEがRADIUSから学習したMACアドレスは特定のSSIDにのみ適用できるため、MDMプロバイダーへのMACアドレスのルックアップが失敗します。
- ISEエンドポイントDB：ランダムなMACアドレスがDBに入力されると、エンドポイントDBは徐々に増加します。ISEは、完全に分散配置されたデータベース内の2.5Mのエンドポイントに制限されます。この制限を超えると、ISEシステムのパフォーマンスに影響が及ぶ可能性があります。

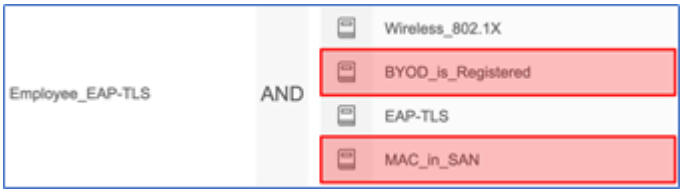
回避策と解決策

現在、サードパーティのMACアドレスのランダム化によって引き起こされる問題に対する大規模な解決策はなく、回避策のみが利用可能です。

注：デバイスレベルでMACアドレスのランダム化を無効にすることができます。そのためには、各エンドユーザデバイスの製造元のマニュアルを参照してください。

個人所有デバイス持ち込み

BYODフローの回避策として、Employee_EAP-TLS許可ルールからMAC_in_SAN条件とBYOD_is_registered条件を削除して、次の図に示すように、証明書を使用してデバイスがSSIDに接続する際にMACアドレスが比較されないようにすることができます。



BYODの詳細については、「追加情報」のセクションを参照してください。

プロファイリングとMDM

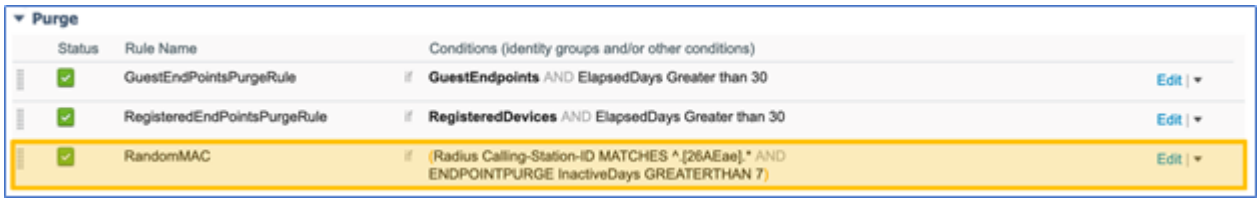
プロファイリングおよびMDMサービスについては、目的のネットワークアクセスを取得する前に、デバイスのMACアドレスのランダム化を無効にするようエンドユーザに指示できます。これを行うには、修正されたホットスポットページにユーザをリダイレクトします。このページでは、デバイスがランダムなMACアドレスを使用してネットワークに接続する際に、MACアドレスのランダム化を無効にする手順が示されます。MACアドレスのランダム化を無効にすると、ユーザは正常に接続できるようになります。詳細については、『ホットスポットポータルを使用した、MACアドレスのランダム化の無効化についてユーザに説明する』を参照してください。

ISEエンドポイントデータベース（オプション）

ISEエンドポイントDBは、時間の経過とともに、未使用のランダムMACアドレスで終了する可能性があります。ISEエンドポイントの消去ポリシーを作成して、ランダムなMACアドレスを定期的に削除し、ISE DBがランダムなMACアドレスで消費されないようにすることができます。

1. Administration > Identity management > Settingsの順に移動します。
2. Endpoint Purgeを選択します。
3. [Purge]セクションで、既存のルールのドロップダウンリスト（[Edit]の横）から、[Insert New Rule ...]を選択します。
4. ルール名としてRandomMACと入力し、次の条件を選択します。
    - Radius:Calling-Station-IDは^.[26AEae].*に一致します。

- ENDPOINTPURGE:7以上の非アクティブ日数



5. [Save] をクリックします。

注：特定の用途に対してランダムなMACアドレスを許可するようにISEが設定されている場合、以前のパージルールでは、過去7日間にネットワークに接続されていないランダムなMACアドレスがすべて削除されます。正当なランダムMACデバイスのパージを回避するには、Never Purgeルールを作成して、該当デバイスをパージルールから除外します。

追加情報

個人所有デバイス持ち込み

Android 10、Android 11、およびApple iOS 14デバイスはランダム化されたMACアドレスを使用するように設定されていますが、ワイヤレスプロファイルがデバイス上で作成される場合、MACアドレスは常に任意のワイヤレスプロファイルに対して同じランダムMACアドレスで生成されます。これは、ワイヤレスプロファイルが削除されて再作成された場合にも当てはまります。ただし、デュアルSSID BYODフローを使用すると、オンボーディングSSIDとセキュアSSIDに異なるMACアドレスが生成されます。これにより、事前に作成されたISE BYOD Employee_EAP-TLS認可ルールを使用する場合にポリシーの不一致が発生します。

これは、以前のバージョンのiOSの実行中にオンボーディングされたデバイスのシングルSSID BYODフローにも影響します。iOS 14より前では、デバイスはワイヤレスアクセスに実際のMACアドレスを使用します。ただし、iOS 14にアップグレードすると、既存のすべてのワイヤレスプロファイルがランダムなMACアドレスを使用するように更新されます。以前のバージョンのiOSとiOS 14以降で使用したMACアドレスが異なるため、MACアドレスに関連する条件をBYODと組み合わせて使用すると、認証が失敗する可能性があります。

詳細情報

この Field Notice に関するご質問などのお問い合せにつきましては、お手数ですが、次のいずれかの方法で シスコシステムズ TAC（Technical Assistance Center）にお問い合せください。

- サービスリクエストをオープン（サービス契約をお持ちの方）
- 電子メールまたは電話で問い合わせる（サービス契約をお持ちでない方）

Field Notice の新着情報を電子メールで受け取るには

My Notifications：プロファイルを設定することにより、ご指定のシスコ製品についての信頼性、安全性、ネットワークセキュリティ、および販売終了（End-of-Sale）などの最新情報を受け取ることができます。

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。