オペレーティングシステムとセキュリティ強化

セキュリティの強化

Unified Communications Manager 12.5SU3 のセキュリティ機能の概要を説明します。以下の項目のいくつかは、シスコの標準製品マニュアルが予定通りに更新される前の項目です。

Unified Communications Manager は、VMware vSphere ESXi に基づく仮想化ハードウェアの最上部で仮想マシンとして実行されます。従来のサーバベースの製品とは異なり、Unified Communications Manager はクローズ系のターンキーパッケージ化された「アプライアンスワークロード」として配布されるソフトウェア製品で、次の特徴があります。

- 攻撃対象領域を縮小します。
- より安定した、より高いパフォーマンスの設定を提供します。
- 設定エラーによる脆弱性を回避します。
- OS/DB のスキルセットが不要で、管理と修正メンテナンスが簡素化されます。

Unified Communications Manager ワークロードレイヤの主なセキュリティ強化は次のとおりです。

- Unified Communications Manager は、汎用/オープンシステムのワークロードではありません。
    - これは汎用の OS 配布を使用しません。
        - 使用されていないモジュールはイメージから除外され、使用されていないサービスは無効化/削除されています。
        - シスコでは、特定のモジュールに対して独自のセキュリティ強化の変更を行います（たとえば、OpenSSL はシスコの Security and Trust Organization によってセキュリティ強化されています）。その結果、CiscoSSL が製品内に組み込まれます。

- ゲスト オペレーティング システム、データベース、ランタイム、その他のワークロード ソフトウェア コンポーネントに対するネイティブインターフェイスは公開されません。
  - これらは、削除または非表示およびロックダウンされます。
  - アクセスは、シスコが提供するブラウザベースの GUI、CLI、または API のみを介して、これらのインターフェイスを保護するさまざまな方法（SSH を介した CLI、またはセキュア FTP を介したファイルのプルなど）を使用して行われます。
- 製品は、注意深く制御されるスタックで構成され、スタックはアプリケーションの操作、保守、保護、および管理に必要なすべてのソフトウェアを含んでいます。シスコは、シスコが提供し、デジタル署名されたイメージを介してすべてのソフトウェアを指定、インストール、および更新します。
- 上記のすべての情報は、ここに記載している Cisco Secure Product Lifecycle 開発アプローチの開発およびテストプロセスの対象となります。
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

- Unified Communications Manager ワークロードレイヤは、上記の制御されたシスコインターフェイスの範囲外の非シスコソフトウェアやソフトウェア更新/変更を挿入することをサポートしません。
  - このワークロード内のすべてのソフトウェアは、シスコによって提供され、デジタル署名され、モノリシックイメージ（.ISO ファイル）として配信されます。
  - ソフトウェアをインストール、アップグレード、および更新するには、シスコが提供する .ISO ファイルまたは .COP ファイルを使用することが唯一の方法です。
  - .ISO ファイルは、シスコイメージ内の 1 つ、一部、またはすべてのソフトウェア要素をインストールまたは更新します。.COP ファイルは、単一の要素、最も一般的なユーザロケールおよび電話機のファームウェアを更新するために使用されます。
  - 以下の設定を有効にすることはできません。
    - ウイルス対策クライアント、UPS エージェント、管理エージェントなどのオンボードエージェント。
    - お客様がアップロード可能または外部でアップロード可能なソフトウェア。
    - サードパーティ製アプリケーション

- ワークロード内のゲスト OS に対する「ルートアクセス」は有効化できません。
  - お客様は、シスコが提供する GUI、CLI、または API で認証を使用します。
  - このワークロードに公開されるインターフェイスはすべて安全です（パスワード複雑性ルールの適用、telnet ではなく SSH、設定可能な最小バージョンの TLS 1.2 など）。

- 通常のGUI/CLI/APIを介してフィールドで修正できない緊急の問題の場合、お客様はシスコ テクニカル アシスタンス センター（TAC）のエキスパートがルートアクセスを取得できるよう、一時的な「リモートアカウント」を設定できます。お客様は制御を維持し、自動的に期限切れとなるこのアカウントをオンまたはオフにできます。お客様は、TAC が実行しているすべてのアクションをログに残した状態で、TAC の担当者が実行している内容を確認することができます。

- 組み込み侵入防御機能：
  - ホストベースの侵入保護機能を提供する、SELinux 適用モード。
    - SELinux 適用モードは、デフォルトで有効になっています。このモードは、アプリケーション、デーモンなどを、ジョブに必要な「最小権限」に制限する必須アクセス制御を適用します。
  - IPTables ホストベースのファイアウォール：
    - IPTables はデフォルトで有効になっています。
    - ルールは、Cisco Service Activationによって調整され、適切なポートが開き、そのサーバで使用されるサービスの正しいレート制限を含んでいます。
    - IPTable ルールは、次のコマンドを使用して表示できます。
      - **utils firewall ipv4 list**
      - **utils firewall ipv6 list**

上記のセキュリティ強化機能に加えて、Unified Communications Manager ワークロードにより、OS、DB、およびアプリケーション ソフトウェアのセキュリティ監査ロギングが実行されます。セキュリティ監査ログには次の 3 種類があります。

- Linux 監査ログ。
- Unified CM アプリケーション監査ログ。
- Informix データベース監査ログ。

また、構成設定では、システム管理者が組織の infosec 要件に準拠するようシステムを設定することもできます。システム管理者が設定可能なセキュリティ設定とユーティリティには、次のものがあります。

- パスワードポリシーの定義。すべてのパスワードとPINはハッシュまたは暗号化され、クリアテキストとして保存されません。
- アカウントのロックアウト設定とログイン情報ポリシー。
- 警告バナーテキスト。
- シグナリングとメディアに対する TLS/SRTP の有効化。
- 電話機のセキュリティ強化設定。

- TLS を使用しない接続を保護するための IPSec。
- 自己署名 PKI 証明書を CA 署名に変更する。
- FIPS モードまたはコモンクライテリアモードの有効化。
- スマートカードまたはバイオメトリック リーダーのサポートを含む SAML シングルサインオンの有効化。
- すべてのネットワーク接続、プロセス、アクティブパッケージを表示します。
  - 「show network status detail all nodns」開いているポートの詳細を取得します。"netstat -an" Unix コマンドに相当します。
  - 「show process list detaill」すべてのプロセスと各プロセスに関する重要な情報のリストを取得します。「ps -ef」Unix コマンドに相当します。
  - 「show packages active」インストール済みおよびアクティブなパッケージの名前とバージョンを表示します。

設定可能なセキュリティオプションの詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。

シスコの UC 製品は、次を含むさまざまな政府認定への準拠について定期的にテストされ、検証されています。

- Department of Defense Information Network Approved Products List（DoDIN APL）
- FIPS 140-2 レベル 1
- FedRAMP
- Common Criteria
- Applicable U.S. Department of Defense Security Technical Implementation Guides（STIGs）

シスコの政府認定の詳細については、次を参照してください。
https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html。

セキュリティ脆弱性アラートと管理のために、Unified Communications Manager ワークロード全体が Cisco Product Security Incident Response Team（PSIRT）によってサポートされます。Cisco PSIRT は、Cisco 製品およびネットワークに関連するセキュリティ脆弱性情報の収集、調査、およびレポートの公開を管理する専門のグローバルチームです。次の操作を実行する必要があります。

- 導入環境に影響を及ぼす可能性があるセキュリティの問題に関するアラートについては、シスコ セキュリティ アドバイザリおよびアラートのページ（https://tools.cisco.com/security/center/publicationListing.x）を参照してください。
- 影響を受ける製品、ワークロード、および永続的な解決策については、 Cisco.com の特定の PSIRT のセキュリティアドバイザリを参照してください。

詳細については、https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。