AT A GLANCE

Secureworks

リモートアクセス脆弱性アセスメント

脆弱性を特定し、新たに拡張されたリモートアクセスインフラストラクチャを狙う攻撃を低減

概要と利点

セキュアワークスのリモートアクセス脆弱性アセスメントは、COVID-19によるリモートワーカーの急増による緊急のセキュリティリスクに対応します。

リモートアクセス脆弱性アセスメントは、広範囲にわたる既存のペネトレーションテストの手法を活用して、組織のリモートアクセスポイントの脆弱性をテストし、新規および既存のリモートアクセステクノロジーがセキュアに導入されていることを検証します。

本サービスの狙いは以下の通りです。

- リモートアクセスセキュリティテスト機能の可用性を促進
- 脅威の攻撃者が一般的に悪用する脆弱性を迅速に可視化
- 攻撃対象領域と侵害のリスクを軽減

Webアプリケーションセキュリティ

Webアプリケーションがリモートアクセス脆弱性アセスメントのスコープ内にあることが判明した場合、セキュアワークスは自動的にWebアプリケーションの非認証スキャンを実行します。Webアプリケーションは、特徴的に最も脆弱なアプリケーションです。Webアプリケーションの完全なテストとアセスメントについては、Webアプリケーションのセキュリティアセスメントをご検討ください。

主な機能

セキュアワークスアドバイザリグループリモートでアクセスメントを行い、リモートワークを中断することなくセキュリティの修復が必要な脆弱性データをご提供します。

テスト計画と検証

- エンゲージメントルール定義のためのキックオフ
- リモートアクセスクライアントまたはプライマリドメインのIPの収集（* 10アドレスまで）
- 外部向けユーザー名・パスワード、ロックアウトポリシーの収集
- スコープの検証により精度を確保し、影響を限定

実行

- OSINT
- オープンサービスを列挙
- オープンネットワークサービスへエクスプロイト
- 非MFAポータルへパスワードスプレー攻撃
- リモートアクセスポイントへの侵害

報告

- エグゼクティブサマリー
- 詳細な調査結果
- テスト実施から1週間以内に結果を納品

リモートアクセスポイントの例

- Citrix
- VDI
- VPN
- Webメールポータル
- リモートデスクトップ（RDP）
- HTTP-NTLM保護サイト（ShareSointやイントラネットなど）

*10リモートアクセスポイントまで。10ポイントを超える場合は、別途ご相談ください。

セキュアワークスについて

グローバルのサイバーセキュリティ・サービス業界をリードする Secureworks®（NASDAQ: SCWX）は、デジタル化が進む社会において、企業組織をサイバーの脅威から保護し続けています。当社は、数千社におよぶお客様から集積したデータと人工知能（AI）、そして独自のカウンター・スレット・プラットフォーム（Counter Threat Platform™：CTP）の自動化による可視性と、お客様の環境を保護する強固なネットワーク効果を創出する当社の卓越したリサーチャーとアナリスト集団から提供される実践的な分析結果を統合してサービスに反映させます。データの種別や出所を問わず集積・分析を行うことで、セキュリティ侵害の防御、悪意ある活動のリアルタイムによる検知、深刻化する脅威の迅速な対応と予見を実現し、サイバーの脅威への対抗策をお客様に提供します。
もっと上手に組み合わせれば、セキュリティは飛躍できる https://www.secureworks.jp/