報道関係者各位

Microsoft Office 365 Message Encryption の脆弱性により メールの内容が漏えいする可能性、ウィズセキュアが警告

～ 修正プログラムが提供されておらず、情報の一部または全体が攻撃者の手に渡ることも ～

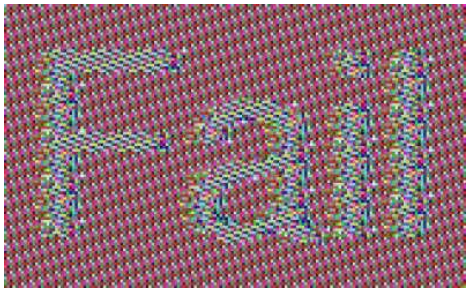
2022 年 10 月 14 日
ウィズセキュア株式会社

先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、同社のセキュリティコンサルタントが Microsoft Office 365 Message Encryption (OME) のセキュリティ上の脆弱性を発見し、この欠陥に関するセキュリティアドバイザリーを公開したことを発表しました。企業が暗号化された電子メールを社内外に送信するために使用する OME は電子コードブック (ECB) モードでの動作を利用していますが、このモードはメッセージの特定の構造情報を漏えいしてしまうことがわかっています。

大規模なメッセージデータベースを持つ攻撃者は、漏えいした情報を使い、個々のメールに繰り返し見られるパターンの位置や頻度を分析し、これらのパターンを他のメールやファイルに見られるパターンと照合することによって、メールの内容を一部または完全に推測することができます。

ウィズセキュアのコンサルタントでこの脆弱性を発見した Harry Sintonen (ハリー・シントネン) は、本件について次のようにコメントしています。
「多数のメッセージを入手した攻撃者は、漏えいした ECB 情報を使って暗号化された内容を把握することができます。メール数が多ければ多いほど、このプロセスは容易かつ正確になるため、攻撃者は、データ漏えい時に盗まれたメールアーカイブを手に入れた後、あるいは誰かのメールアカウントやメールサーバーに侵入したり、バックアップにアクセスしたりすることで実行することができます。」

本件に関するアドバイザリーでは、電子メールの分析はオフラインで行うことができ、攻撃者が過去のメッセージのバックログやアーカイブを侵害する可能性があると指摘しています。その際、企業には電子メールを入手した攻撃者が Sintonen が指摘する方法を使用して、メールの内容が読み取られてしまうことを防ぐ方法がありません。また、このアドバイザリーでは、解析を行う際には暗号鍵の知識が不要であること、BYOK (Bring Your Own Key) 方式を使用しても問題が改善されないことを強調しています。



(Office 365 Message Encryption で保護されたメールから抽出された画像)

Sintonen は、2022 年 1 月にマイクロソフト社にリサーチの内容を報告し、同社はこの問題を認め、脆弱性報奨金プログラムを通じて Sintonen に報奨金を支払いましたが、修正プログラムを発行しないことを選択しました。企業は、OME を使用しないことで問題を軽減させることができますが、攻撃者が OME で暗号化された既存の電子メールにアクセスするリスクには対処することができません。
「OME を使用して電子メールを暗号化していた企業は、基本的にこの問題を回避することができません。契約や GDPR のような規制で守秘義務を課せられているような企業では、この問題が発生する可能性があります。そしてもちろん、このデータが実際に漏えいした場合の影響も企業にとっては大きな懸念材料となります。」
と、Sintonen は締めくくっています。

マイクロソフト社からの修正プログラムもなく、メール管理者やユーザーが利用できるより安全な操作モードもないため、ウィズセキュアでは、メールの機密性を確保する手段として OME の使用を避けることを推奨しています。

(実際の個々の画素の値は不明であるものの、実際の画像内容は容易に特定可能)

本件に関するアドバイザリー (日本語) の全文は以下のページでご覧いただけます。
https://www.withsecure.com/content/dam/with-secure/ja/resources/20221014_WithSecure_Office365_Advisory_JP.pdf

WithSecure Web サイト:
https://www.withsecure.com/jp-ja/
WithSecure プレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

WithSecure™は、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立された WithSecure は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。