WithSecure セキュリティアドバイザリー

Microsoft Office 365 メッセージ暗号化の安全でない動作モードについて

発行日:
2022 年 10 月 14 日

タイプ:
不完全または危険な暗号アルゴリズムの使用

深刻度:
高

対象製品:
Microsoft Office 365

対応策:
マイクロソフトはこの脆弱性を修正する予定はないため、Microsoft 365 Message Encryption の使用を避けることが唯一の対応策となります。

クレジット:
WithSecure Consulting の Harry Sintonen による脆弱性の発見

レファレンス:
msrc vuln-060517

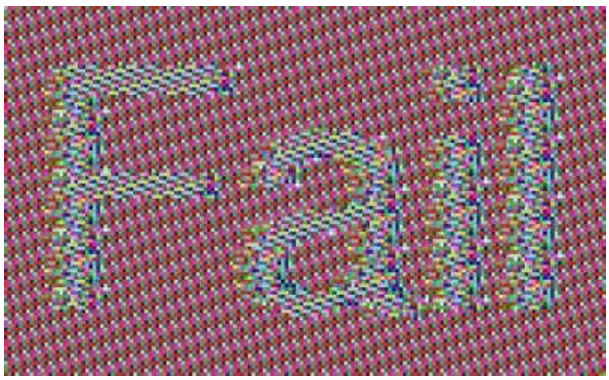
時系列での経緯:
2022-01-11
脆弱性を発見し、MSRC 経由で VULN-060517 として脆弱性を報告
2022-01-19
マイクロソフトより 5,000 米ドルの報奨金を受領
2022-05-19
マイクロソフトに問題の状況について問い合わせたが、返信なし

2022-08-29
マイクロソフトに対し、本脆弱性を公開予定である旨を通知
2022-09-21
マイクロソフトより、本件について以下の回答あり
「本レポートは、セキュリティサービスの要件を満たしておらず、漏えいともみなされません。コードの変更も行われていないため、このレポートに対して CVE は発行されませんでした。」
2022-10-14
WithSecure よりセキュリティアドバイザリーを発表

概要:
Microsoft Office 365 メッセージ暗号化 (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。このモードは一般的に安全ではなく、送信されたメッセージの構造に関する情報が漏えいし、その結果メッセージの一部または全体が明らかになってしまう可能性があります。NIST の "Announcement of Proposal to Revise Special Publication 800-38A "には「"NIST National Vulnerability Database (NVD) において、機密情報を暗号化するための ECB モードの使用は、深刻なセキュリティ脆弱性引き起こす可能性があります。一例として CVE-2020-11500 を参照してください。」との記載があります。

説明:
Microsoft Office 365 は、暗号化されたメッセージを送信する方法を提供しています。この機能は、組織内外の人と暗号化された電子メールメッセージを安全な方法で送受信できるようにすることをうたっています。しかし、OME メッセージは、安全ではない ECB モードで暗号化されています。

影響:
ECB モードがメッセージの特定の構造情報を漏えいさせるため、暗号化された電子メールにアクセスできる悪意のある第三者がメッセージの内容を特定することができるようになり、それにより機密性が損なわれる可能性があります。


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

暗号化されたメッセージは、通常の電子メールの添付ファイルとして送信されるため、送信されたメッセージは様々な電子メールシステムに保存され、送信者と受信者の間の不特定多数の人々に傍受される可能性があります。

大規模なメッセージデータベースを持つ攻撃者は、傍受したメッセージの繰り返し部分の相対的な位置を分析することで、メッセージの全体または一部を推測することができます。

ほとんどの OME 暗号化メッセージが影響を受け、過去に送信／受信／傍受された暗号化メッセージに対してオフラインで攻撃を行うことが可能です。すでに送信されたメッセージの解析を防ぐ方法はなく、権限管理機能を使用して問題を解決することもできません。

暗号化されたメッセージで送信される内容によっては、この脆弱性の法的影響を考慮する必要がある企業も出てきます。EU 一般データ保護規則 (GDPR)、カリフォルニア州消費者プライバシー法 (CCPA)、またはその他の類似の法律に記載されているように、脆弱性がプライバシーに影響を与える可能性があります。

詳細:

ECB モードとは、各暗号ブロックが個別に暗号化されることを意味します。平文メッセージのブロックの繰り返しは、常に同じ暗号文ブロックに対応します。これは、実際の平文が直接明らかにされない一方で、メッセージの構造に関する情報が明らかにされることを意味します。以下は、ECB モードで AES 暗号化された元画像です。

(実際の個々の画素の値はわからないが、実際の画像内容は容易に特定可能)

このように、特定のメッセージが直接情報を漏らすことはなくても、大規模なメールデータベースを持つ攻撃者は、ファイル内で繰り返されるパターンの関連性を分析し、特定のファイルを特定することができます。これにより、暗号化されたメッセージの全体または一部を推測することができるようになる可能性があります。

この脆弱性の悪用は暗号鍵の知識を必要としないため、BYOK (Bring Your Own Key) や同様の暗号鍵の保護対策は改善効果がありません。

Microsoft Office 365 Message Encryption に使用されている暗号は、Advanced Encryption Standard (AES) であるようです。しかし、本脆弱性の文脈においては、ECB の動作モードは使用される暗号に関係なく同じ特性を持つため、実際の暗号は関係ありません。

CWE-327: 不完全または危険な暗号化アルゴリズムの使用

Outlook 365 のメッセージ暗号化では、メッセージを RPMSG に暗号化する際に、ECB モードの操作を使用します。

脆弱性の根本的な原因は、メッセージの暗号化で ECB モードを使用することを事前に決定し、その誤った決定で互換性を維持したことにあると思われます。

Microsoft Information Protection (MIP) ProtectionHandler::PublishingSettings クラスには、SetIsDeprecatedAlgorithmPreferred メソッド (1) があり、次のように記載されています。

"後方互換性のために非推奨の暗号アルゴリズム (ECB モード) を優先するかどうかを設定する。"

OME は、RPMSG の ECB 暗号化を有効にするために、この方法を使用していると思われます。このフラグが設定されていない場合、Cipher Block Chaining (CBC) モードが使用されます。

Microsoft Information Protection FIPS 140-2 Compliance (2) のドキュメントには、次のような記載があります。

"Office のレガシーバージョン (2010) は AES 128 ECB を必要とし、Office ドキュメントは今でも Office アプリによってこの方法で保護されています。"

改善について:

マイクロソフトに対して脆弱性の状況について何度も問い合わせをしましたが、最終的には以下のような回答がありました。

「本レポートは、セキュリティサービスの要件を満たしておらず、漏えいともみなされませんでした。コード変更も行われなかったため、本件に対して CVE は発行されませんでした。」

エンドユーザーまたはメールシステムの管理者には、より安全な操作モードを強制するオプションはありません。マイクロソフトはこの脆弱性を修正する予定がないため、唯一の対応策は、Microsoft Office 365 Message Encryption の使用を避けることであると言えます。