プレスリリース
報道関係者各位

2018 年 9 月 6 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、ファクス機を乗っ取り、
ネットワーク侵入やマルウェア感染を可能にする「ファクスプロイト」攻撃手法を発見
世界中の企業や家庭で使用されている数千万台のファクス機に影響する脆弱性、
不正なファクスを送信するだけでネットワークのハッキングが可能に

米カルフォルニア州 サン カルロス - 2018 年 8 月 13 日

ゲートウェイからエンドポイントまで、包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ(Check Point® Software Technologies Ltd. NASDAQ: CHKP）は本日、世界中の数千万台のファクス機で採用されている通信プロトコルの脆弱性を悪用し、ネットワークをハッキングできることを発見したと発表しました。この脆弱性は、標的のファクス番号を知っているだけで悪用でき、攻撃を受けた場合、企業や家庭のネットワークを乗っ取られるおそれがあります。

チェック・ポイントの研究者は、広く使用されている HP 製のファクス複合機 Officejet Pro でこの脆弱性を悪用できることを実証しました。問題のプロトコルは、HP 以外にも多くのメーカーのファクス機や複合機、さらには fax2email などのオンライン・ファクス・サービスで使用されており、いずれも同じ攻撃手法による影響を受けると考えられます。なお、チェック・ポイントの研究者は、同脆弱性を発見後、HP に情報を提供しています。同社は、影響を受ける複合機用のソフトウェア・パッチを直ちに開発し、HP.com で公開しています。

現在、コミュニケーション手段として主流ではなくなりつつありますが、今日でも、世界中の企業で 4,500 万台以上のファクス機が稼働しており、1 年あたり 170 億枚ものファクスが送受信されています。特に広く使用されているのは、ヘルスケアや法律、銀行、不動産など、機密性の高い個人情報を大量に扱う業種の組織です。例えば、英国の国民保健サービスだけでも 9,000 台以上のファクス機を所有し、日常的に患者情報を送受信しています。また多くの国では、電子メールが裁判の証拠として認められておらず、特定の業務処理や法務処理でファクスが使用されています。売上を見ても、ヨーロッパで販売されるレーザー・プリンタの半数近くは、ファクス機能を搭載する複合機となっています。

チェック・ポイントのセキュリティ・リサーチ担当グループ・マネージャのヤニブ・バルマス（Yaniv Balmas）は、「ファクス機が自社のネットワークに接続されていることにさえ気づいていない企業は少なくありません。しかし、多くの複合機や個人向けプリンターはファクス機能を搭載しています。今回の調査では、ファクス機という意外な機器がサイバー犯罪者にハッキングされ、ネットワークへの侵入やデータ侵害、業務妨害に悪用される可能性が明らかになっています」と述べています。

「ファクス機を所有する企業各社は、この攻撃からネットワークを保護するため、最新のパッチを適用したうえで、ファクス機をネットワーク上の他のデバイスから切り離す必要があります。高度で複雑な第 5 世代のサイバー攻撃が蔓延する今日、ネットワークのいかなる部分も、セキュリティをおろそかにすることはできません」（バルマス）

この脆弱性の悪用は、企業 Web サイトなどで公開されている標的のファクス番号を入手し、特別な細工を施した画像ファイルをファクス機に送信するだけで可能となります。ランサムウェアや仮想通貨のマイニング・ツール、スパイウェアなどのマルウェアを画像ファイルに埋め込み、標的のファクスに送信すると、マルウェアをファクス機にデコードさせ、メモリに格納できます。そして、ファクス機が接続されたネットワークにマルウェアを送り込むことで、機密データを窃取したり業務を妨害したりできるという仕組みです。

セキュリティ・リスクを最小限に抑えるため、チェック・ポイントでは、使用しているファクス機に新しいファームウェアが公開されていないかどうかを確認し、直ちに適用することを推奨します。また、機密情報を扱うアプリケーションやサーバとは別の安全なネットワーク・セグメントにファクス機を設置することを検討してください。ファクス機を他のデバイスから切り離しておくと、ネットワーク全体へのマルウェアの拡散を抑制できます。

チェック・ポイントの研究者であるバルマスとエヤル・イトキン（Eyal Itkin）は、セキュリティとハッキングに関する主要カンファレンス DEF CON 26 でこの脆弱性を発表しました。今回の発見の詳細については、チェック・ポイントのコーポレート・ブログをご覧ください。チェック・ポイントの研究者による本脆弱性の詳細な解説については、チェック・ポイントのリサーチ・ブログをご覧ください。

本リリースは、米国時間 8 月 13 日に配信されたものの抄訳です。

日本語リリース本文はこちらをご確認ください。
https://www.checkpoint.co.jp/press/2018/pressrelease_20180906.html

■チェック･ポイントについて

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、世界各国の政府機関や企業など、あらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供する大手プロバイダーです。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェアなどの多岐にわたる第 5 世代のサイバー攻撃から保護します。企業のクラウドやネットワークのほかモバイル・デバイスに保存されている情報を、今日の第 5 世代のサイバー攻撃を含めてあらゆる脅威から保護するため、第 5 世代の脅威に対応するマルチレベルのセキュリティ・アーキテクチャを備え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社　広報代行　共同ピーアール株式会社

担当　マーケティング　横山

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: marketing_jp@checkpoint.com

担当　上瀧・花岡

Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

