プレスリリース
報道関係各位

2019 年 8 月 14 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・ポイントの調査で、Wi-Fi 接続対応の最新のカメラにランサムウェアやマルウェアに対する脆弱性の存在が判明

写真を人質に身代金を要求されるおそれのある重大な脆弱性を特定

米カルフォルニア州サンカルロス ― 2019 年 8 月 11 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）の脅威情報部門である Check Point Research は本日、最新のカメラにおいて USB や Wi-Fi 接続経由のランサムウェア攻撃、マルウェア攻撃に対する脆弱性が見つかったことを発表しました。

最近のカメラはキャプチャや再生にフィルムを使用していないため、国際映像産業協会はカメラから PC にデジタル画像を転送する標準プロトコルとして PTP（画像転送プロトコル）を考案しました。当初は画像転送専用でしたが、今ではライブ配信からファームウェアのアップグレードまで様々な用途に対応するコマンドが多数追加されています。

Check Point Research は、カメラのプロトコルの脆弱性を悪用して、ランサムウェアの感染に成功するか調査を実施しました。この調査では、USB と Wi-Fi の両方に対応し、PTP で重大な脆弱性が見つかっているキヤノンのデジタル一眼レフカメラ EOS 80D を使用。チェック・ポイントでは、PTP が標準のプロトコルで他のブランドでも利用されていることから、他社のカメラでも同様の脆弱性が見つかる可能性があると考えています。

チェック・ポイントのセキュリティ研究者であるエヤル・イトキン（Eyal Itkin）は、「デジタル一眼レフカメラに限らず、どのスマート・デバイスも攻撃と無縁ではありません。現在のカメラは USB 接続に止まらず、Wi-Fi ネットワークや周囲の環境との接続も可能となっています。攻撃者がカメラや接続先の PC にランサムウェアを挿入できる状況であり、脅威に対する脆弱性はますます高まっていると言えるでしょう。写真を人質として、身代金を要求される事態も考えられます」と述べています。

カメラへの感染を防ぐ方法:

1. 最新のファームウェアを適用し、パッチが公開されている場合はインストールします。
2. 不要なときには Wi-Fi 接続をオフにします。
3. Wi-Fi 使用時には、公共の Wi-Fi ネットワークに接続せずカメラを Wi-Fi アクセス・ポイントとして使用します。

Check Point Research は、確認された脆弱性とパッチの適用で連携した企業について既にキヤノンに情報を提供しています。キヤノンは公式のセキュリティ勧告を英語と日本語で発表し、パッチも公開しています。

今回の調査の実施方法について詳しくは、こちら https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera またはこちら https://youtu.be/75fVog7MKgg をご覧ください。

本リリースは 8 月 11 日に英文で出されたものの抄訳です。原文はこちらをご覧ください。
https://www.checkpoint.com/press/2019/check-point-research-reveals-modern-cameras-connectivity-to-wi-fi-make-them-vulnerable-to-ransomware-and-malware/

■Check Point Research について

Check Point Research は、チェック・ポイントの顧客やインテリジェンス・コミュニティ全般に向けて、業界有数のサイバー脅威情報を提供しています。世界中で発生しているサイバー攻撃に関する情報を ThreatCloud に蓄積して分析し、ハッカーを追跡しながら、チェック・ポイントの各製品に搭載される最新の保護機能の開発に携わっています。Check Point Research は、セキュリティ・ベンダー各社や捜査当局、各種 CERT と協調する 100 人以上のアナリストと研究者で構成されています。

■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（https://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、高度な標的型の脅威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、モバイル・デバイスを、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「Infinity Total Protection」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》
広報代行　共同ピーアール株式会社
担当　上瀧・花岡
Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

