2017 年 11 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、LG 製スマート家電の脆弱性「HomeHack」修正に協力

LG SmartThinQ®スマート家電の深刻なセキュリティ脆弱性に対処

ゲートウェイからエンドポイントまでの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・テクノロジーズ株式会社（本社：東京都、代表取締役社長：ピーター・ハレット、以下チェック・ポイント）は本日、チェック・ポイントのセキュリティ研究者が、数百万ユーザが利用する LG 製スマート家電 LG SmartThinQ®アプリの脆弱性「HomeHack」を発見したと発表しました。この脆弱性が悪用された場合、LG 製スマート家電製品が不正に遠隔制御される恐れがあります。

今回発見された脆弱性は、LG SmartThinkQ のモバイル・アプリおよびクラウド・アプリケーションに存在します。チェック・ポイントの調査チームが確認したところ、この脆弱性を悪用すると、SmartThinkQ クラウド・アプリケーションにリモートからログインし、ユーザの正規の LG アカウントを乗っ取り、ロボット掃除機とその内蔵ビデオ・カメラを制御できるようになります。LG アカウントを乗っ取られた場合、そのアカウントに関連付けられた LG 製の各種デバイスや家電製品（ロボット掃除機、冷蔵庫、オーブン、食器洗い機、洗濯機、ドライヤー、エアコンなど）を攻撃者に制御される可能性があります。

HomeHack を悪用する攻撃者は、ロボット掃除機 Hom-Bot の内蔵ビデオ・カメラを利用して、ユーザの日常生活を盗み見する可能性があります。Hom-Bot 内蔵カメラが、HomeGuard Security 機能の一部として、関連付けられた LG SmartThinkQ アプリにライブ映像を送信する機能が悪用されます。また、同じ宅内で LG 製の食器洗い機や洗濯機が使用されている場合は、その電源も攻撃者に操作される可能性があります。

チェック・ポイントの検証では、この脆弱性利用により、偽の LG アカウントを作成して正規の LG アカウントを乗っ取り、そのユーザの LG 製スマート家電を遠隔制御できることが確認されています。チェック・ポイントは、2017 年 7 月 31 日、責任ある開示ガイドラインに則り、この問題を LG に報告しました。これを受けて LG は、9 月末に SmartThinkQ アプリケーションの問題を修正しています。

LG の SmartThinQ モバイル・アプリと家電製品を利用しているユーザは、デバイスを保護するため、LG の Web サイトから提供されている最新のソフトウェア・バージョンにアップデートする必要があります。チェック・ポイントでは、スマート家電やホーム Wi-Fi ネットワークへの侵入と遠隔制御を防止するため、以下の対策の実施を推奨しています。

1. LG SmartThinQ を最新バージョン（V1.9.23）にアップデートしてください。アップデートは、Google Play、Apple App Store、または LG SmartThinQ アプリの設定画面から実行できます。

2. スマート家電を最新バージョンにアップデートしてください。SmartThinQ アプリケーション・ダッシュボードにある該当のスマート家電をクリックして実行できます（アップデートが存在する場合、ポップアップ・メッセージが表示されます）。

チェック・ポイントの製品脆弱性調査担当責任者であるオーデッド・ヴァヌヌ（Oded Vanunu）は、「LG 社は、SmartThinkQ アプリおよびデバイスの問題を修正する適切な対応を、責任を持って遂行しました。家庭用スマート・デバイスが今後さらに普及すると、攻撃者の狙いは、個々のデバイスではなく、そのネットワークを管理するアプリに移るでしょう。ソフトウェアの不備に付け込む方が、効果的に脆弱性を悪用でき、家電を暴走させたり、機密データにアクセスしたりするのも容易だからです。IoT デバイスを使用するユーザは、セキュリティやプライバシー上のリスクに目を向ける必要があります。メーカーは、ソフトウェアやデバイスの設計段階で堅牢なセキュリティを組み込み、スマート・デバイスに対する攻撃に備えることが必須です」と述べています。

LG Electronics 社のスマート・ソリューション BD、スマート開発チームのマネージャを務めるクンソク・リー（Koonseok Lee）氏は、「LG Electronics では、世界中の人々の暮らしを豊かにするというミッションの一環として、次世代スマート家電ラインナップの拡充を進めています。同時に、ソフトウェア・プログラムの安全性と信頼性を高めることにも重点を置いています。今年 8 月、LG Electronics は、セキュリティ問題を確認するため、チェック・ポイント・ソフトウェア・テクノロジーズ社と協力して、root 化を伴う高度な検証作業を実施するとともに、直ちにパッチ・プログラムの開発に着手しました。当社のセキュリティ・システムでは、9 月 29 日より、問題を解決したバージョン 1.9.20 が動作しています。LG Electronics では、ソフトウェア・セキュリティ・システムの継続的な強化に努めるとともに、チェック・ポイント社をはじめとするサイバー・セキュリティ・ソリューション・プロバイダと協力して、安全性と利便性を高めた家電製品の開発に取り組んでいきます」と述べています。

SmartThinQ®の幅広いスマート家電および監視ソリューションでは、スマートフォンから自宅内の様子を監視、管理できます。ロボット掃除機の Hom-Bot は、2016 年上半期に 40 万台以上を売り上げています。同年におけるスマート家電の世界出荷台数は、2015 年比で 64%増となる 8,000 万台に達しています。

攻撃の手口を紹介した動画をこちらからご覧いただけます。

この脆弱性の詳細については、チェック・ポイントのブログ（英文）をご覧ください。

■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しています。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保護するマルチレベルのセキュリティ・アーキテクチャに加え、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。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、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（ http://www.checkpoint.co.jp/ ）は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

####

《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

担当　マーケティング　宮

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

広報代行　共同ピーアール株式会社

担当　花岡・上瀧

Tel: 03- 3571－5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp

