プレスリリース
報道関係各位

2019 年 6 月 27 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・ポイントのリサーチ・チームと CyberInt、Electronic Arts のゲーム・クライアント「Origin」に深刻な脆弱性を発見

世界中の 3 億人以上の EA ゲーム・ユーザが、アカウント乗っ取りや
個人情報窃取の被害に遭うおそれがあった重大な脆弱性

米カルフォルニア州サンカルロス/テルアビブー 2019 年 6 月 26 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 と、脅威を検出および緩和するマネージド・サービスをデジタル企業向けに提供する大手サイバー・セキュリティ・プロバイダの CyberInt は本日、Electronic Arts（EA）が開発したゲーム・クライアント「Origin」に一連の脆弱性を発見したと発表しました。すでに修正済みのこれらの脆弱性が放置されていた場合、プレイヤー・アカウントの乗っ取りや個人情報の窃取などの被害が生じる可能性がありました。

世界第 2 位のゲーム会社である EA は、「FIFA」、「Madden NFL」、「NBA Live」、「UFC」、「The Sims」、「Battlefield」、「Command and Conquer」、「Medal of Honor」など、著名な家庭用ゲーム作品を数多く保有しています。これらのゲームでは、PC とモバイル・デバイスを横断して EA のゲームを購入、プレイできるクライアント向けゲーム・プラットフォームの Origin を利用します。Origin は、ゲーム機能だけでなく、プロフィール管理やチャットによる交流機能、直接ゲーム参加などのソーシャル機能を備えるほか、Facebook、Xbox Live、PlayStation Network、Nintendo Network などのコミュニティ・サイトとも統合されています。

CyberInt とチェック・ポイントの研究者は、攻撃グループに悪用される前に EA が脆弱性を修正し、アップデートを配信できるよう、協調的な脆弱性情報開示プロセスに従い、責任を持って EA に問題を報告しました。そのうえで、ゲーム・ユーザを確実に保護すべく、アップデートの開発に際しても EA に協力しています。すでに脆弱性は修正されていますが、問題が放置されていた場合、プレイヤーのセッションをハイジャックされ、アカウントの侵害や乗っ取りなどの被害が生じていた可能性があります。

EA でゲームおよびプラットフォーム・セキュリティ担当シニア・ディレクターを務めるエイドリアン・ストーン（Adrian Stone）氏は、「当社にとって、ユーザの保護は非常に重要な問題です。CyberInt とチェック・ポイントからの連絡を受け、私たちは、社内の製品セキュリティ対応プロセスに従い、報告された問題を修正しました。協調的な脆弱性情報開示方針の下、各社が協力することは、当社とサイバー・セキュリティ・コミュニティとの関係を強化するものであり、ユーザを保護するうえで重要な役割を担っています」と述べています。

今回見つかった脆弱性を悪用するために、ユーザのログイン情報を入手する必要は一切ありません。脆弱性の悪用では、破棄されたサブドメインと、EA Games のユーザ・ログイン・プロセスに組み込まれた OAuth によるシングル・サインオン（SSO）および信頼メカニズムに関係する認証トークンを使用します。

チェック・ポイントの製品脆弱性調査担当責任者を務めるオーデッド・ヴァヌヌ（Oded Vanunu）は、「EA の Origin は、非常にポピュラーなゲーム・プラットフォームです。もし今回の脆弱性が修正されないまま放置されていた場合、膨大なユーザ・アカウントが乗っ取られ、悪用された可能性があります。チェック・ポイントは先ごろ、Epic Games がゲーム作品『フォートナイト』向けに運用しているプラットフォームにも脆弱性を発見していますが、この 2 つの問題は、オンライン・アプリケーションやクラウド・アプリケーションがサイバー攻撃やセキュリティ侵害に対していかに脆弱であるかを物語っています。このところ、ゲーム・プラットフォームが攻撃者に狙われるケースが増えているのは、これらのプラットフォームが重要性の高い個人情報を大量に保有していることが理由です」と述べています。

CyberInt Technologies の共同創業者で戦略担当シニア・バイスプレジデントを務めるイテイ・ヤノフスキー（Itay Yanovski）氏は、「CyberInt では、攻撃者の意図を理解しながら、継続的、自動的、かつ早期に脅威を検出することによって、企業各社が顧客や事業をプロアクティブに保護できるよう支援しています。ゲーム内アイテムは、公式のマーケットプレイスだけでなく、ダークネットの非公式マーケットでも取引されるほどの人気があります。つまり攻撃者にとって、ゲーム会社は非常に見返りが大きい標的なのです。サイバー・セキュリティ業界は、人々を保護する責任を負っていると私たちは考えています。そのため当社では、先日の TA505 など、新たに見つかった攻撃キャンペーンに関する脅威調査レポートを通じてセキュリティ関係者に警鐘を鳴らし、組織や個人が効果的な検出手法や対策手法を導入できるようにしています」と述べています。

チェック・ポイントと CyberInt は、ゲーム・ユーザに対し、2 ファクタ認証を使用するとともに、ゲームのダウンロードや購入は公式 Web サイト以外からは行わないことを強く推奨します。保護者の方は、お子様に対し、インターネットにはオンライン詐欺の危険があること、サイバー犯罪者は個人情報や金融情報（これらはゲームのアカウント情報に関連付けられている場合があります）を窃取するためにあらゆる手段を講じてくることを教えるようにしてください。また、見知らぬ相手から送られてきたリンクをむやみに開かないようにすることも大切です。

本脆弱性の詳細な技術分析については、Check Point Research のブログをご覧ください。
同脆弱性の特徴について詳しく解説した公式の動画もご覧ください。

本リリースは、米国時間 6 月 26 日に配信されたものの抄訳です。

■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。

■CyberInt Applied Research について

CyberInt Applied Research は、各地域の幅広い業種に対する脅威に着目しながら、攻撃者のスパイ活動や戦術、技術、手順（TTP）を調査しています。最新の脅威や攻撃グループを追跡し、その能力や活動についての情報を提供しています。

■CyberInt について

CyberInt（www.cyberint.com）は、ビジネス視点のアジャイルな知見とアクションを基に、サイバー・セキュリティをビジネスの競争力へと転換します。サイバー・セキュリティの専門知識とビジネスに対する深い理解を組み合わせた業界唯一のプラットフォームを通じて、企業にとって最も重要な要素、つまりビジネス目標、顧客、社員、そしてブランドを保護する知見とアクションを提供します。CyberInt は、世界各地の大手小売企業や金融サービス企業、ゲーム会社を顧客としており、各業種に固有の脅威、ニーズ、特性を深く理解しています。

CyberInt の中核をなす CyberInt Applied Research は、各地域の幅広い業種に対する脅威に着目しながら、攻撃者のスパイ活動や TTP を調査しています。最新の脅威や攻撃グループを追跡し、その能力や活動についての情報を提供しています。

《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

