【ニュースリリース】

2024 年　7 月　5 日

株式会社サイバーセキュリティクラウド

報道関係者各位

【注意喚起】PHP の脆弱性を狙った攻撃が 6 月 7 日以降で約 10 倍に急増！ ダークウェブへの不用意なアクセスにもご注意を

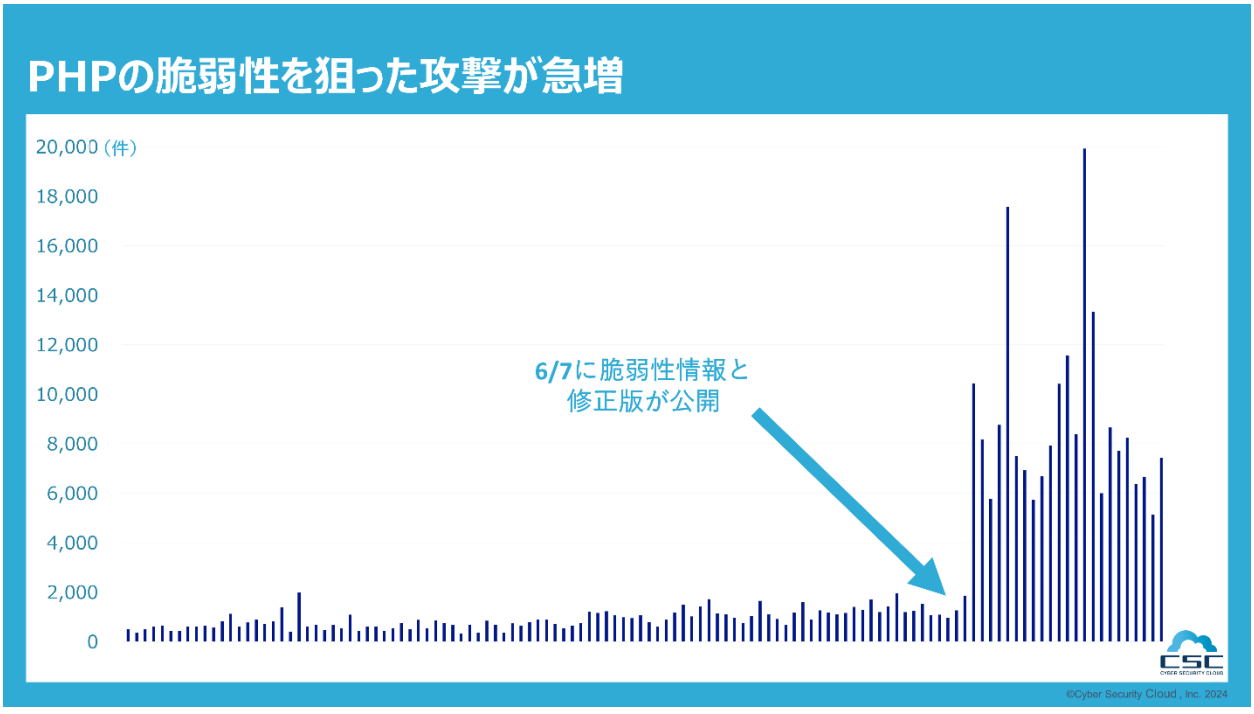
グローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長兼 CEO：小池 敏弘、以下「当社」）は、日本国内 24,000 以上のサイトを対象とした調査で、6 月 7 日以降に PHP CGI の脆弱性（CVE-2024-4577）を狙ったサイバー攻撃が急増していることを確認いたしました。早急に対応が必要な「脆弱性」と、「ダークウェブ」への不用意なアクセスについて注意喚起し、被害に合わないための対策やダークウェブの危険性についてお知らせします。

«サマリー»

・PHP の脆弱性を狙った攻撃が 6 月 7 日以降で約 10 倍に急増！

・ダークウェブへの不用意なアクセスにもご注意を

【PHP の脆弱性を狙った攻撃が 6 月 7 日以降で約 10 倍に急増！】



▲当社が検知した攻撃数の推移

調査によると、PHP の脆弱性（CVE-2024-4577）を悪用した攻撃は 6 月 7 日以降、急激に増加しています。直近 3 ヶ月の平均と比べて最大 10 倍もの攻撃が検知されており、多くの Web サイトが攻撃のリスクに晒されています。この脆弱性を利用したマルウェアの存在も確認しており、ランサムウェアとしてすでに被害が発生してもおかしくありません。企業サイトや個人情報を扱うサイトは脆弱性を放置せず早急な対策が必要です。

■PHP の脆弱性（CVE-2024-4577）とは

PHP の CGI モードにおいて攻撃者が特定の入力を利用して任意のコードを実行できる問題です。これは、PHP が入力値を適切に処理しないために発生し、Windows OS 上で動作するすべての PHP バージョンが影響を受けます。この脆弱性を悪用することで、攻撃者はリモートでサーバー上のコマンドを実行し、システムに深刻な影響を及ぼす可能性があります。対策として、PHP の最新バージョンへのアップデートが推奨されます。

PHP：PHP は、主に動的な Web ページを作成するために利用されるプログラミング言語です。例えば、ユーザーがログインすると、そのユーザーの情報を表示するページを動的に生成するのに PHP が使われます。

CGI（Common Gateway Interface）：CGI は、Web サーバーが PHP など外部のプログラムと連携するための仕組みです。例えば、ユーザーが Web サイトに情報を入力して送信したときに、その情報をサーバー側で処理するために CGI が使われます。

【ダークウェブへの不用意なアクセスにもご注意を】

また昨今、ダークウェブの存在がニュース等で取り上げられることが増えており、不用意にダークウェブにアクセスされている様子が散見されています。これは非常に危険な行為です。そこで、ダークウェブの危険性についても併せてお知らせいたします。

■ダークウェブとは

一般的な検索エンジンではアクセスできないインターネットの一部です。特定のソフトウェア、設定、認証が必要で、匿名性を提供するために設計されたネットワークのことを指します。

【本件に関するお問い合わせ】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

■ダークウェブについてのよくある誤解と注意喚起

ダークウェブに関する誤解も多く存在しますが、ダークウェブは非常に危険な場所であり、一般ユーザーが安易にアクセスすることは推奨されません。リスクを理解し、安全性を最優先に考えた行動を心がけてください。

安全性の誤解:

ダークウェブには多種多様なコンテンツがあり、攻撃を目的としたサイトも多く存在します。不用意にアクセスすることで、個人情報の漏洩やマルウェア感染のリスクが高まります。

合法と違法の混同:

一部の合法的な利用方法もありますが、違法な取引や活動が盛んに行われているため、不用意なアクセスが意図せず犯罪に関与する可能性があります。

匿名性の誤解:

多くの人はダークウェブが完全に匿名だと思われるかもしれませんが、実際には高度な監視技術が存在し、追跡されるリスクがあります。また、不用意に流出データをダウンロードすることは、犯罪グループの利益に繋がりますので興味本位でデータの購入やダウンロードは絶対にしないでください。

【本件に関するお問い合わせ】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

■当社 CTO 渡辺洋司が提唱する企業が取り組むべき３つの対策

1.技術的対策

技術的な対策として、まずはセキュリティ製品の導入や、侵入を防ぐ取り組みを実施することです。また、実施すべき対策を出来うる限りリストアップして可視化することも大切です。全ての対策を即時に実行できない場合もあるので、必要最低限手をつけることができるものから対策を始めましょう。社内でどの対策を実施できるか議論を重ねることで、サイバーセキュリティ対策における問題を再認識することもできます。

＜技術的対策の例＞

PC へのウイルス対策ソフトの導入、IDS/IPS の導入、WAF の導入

使用しているソフトウェアの定期的な更新、セキュリティ診断の実施

脆弱性を出さないことを意識したシステム作り

2.物理的対策

物理的対策とは、盗難・災害といった物理的要因に対する対策を指します。

実際に起こりえるかはわかりませんが、万が一のことを想定して、対策を行いましょう。

＜物理的対策の例＞

防犯カメラの設置、社員デスクの施錠徹底、オフィスの施錠徹底、入退室記録の管理

生体認証システムの導入、耐震強化、耐震設備の導入

【本件に関するお問い合わせ】

株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑

TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997

E-Mail：pr@cscloud.co.jp

3.人的対策

人的な対策はセキュリティに対してのルールを設定する対策です。またルールを設定するだけでなく、社員に遵守してもらうように説明会などの教育も併せて重要となります。

＜人的対策の例＞

業務の持ち帰りの制限、パスワード管理のルール決め、標的型メールについての教育

セキュリティ教育の実施、インシデント発生時の連絡・報告体制の決定

技術・物理・人の 3 つの対策を実施することでより安全性を高めることができるでしょう。

■株式会社サイバーセキュリティクラウドについて

会社名：株式会社サイバーセキュリティクラウド

所在地：〒141-0021　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階

代表者：代表取締役社長 兼 CEO 小池敏弘

設立：2010 年 8 月

URL：https://www.cscloud.co.jp

「世界中の人々が安心安全に使えるサイバー空間を創造する」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使した Web アプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの 1 つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【本件に関するお問い合わせ】

株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑

TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997

E-Mail：pr@cscloud.co.jp