News Release

報道関係者各位

ニュースリリース

平成 30 年 4 月 19 日

株式会社サイバーセキュリティクラド

Drupal 脆弱性を突いた攻撃が急増

脆弱性を悪用する概念実証(PoC)コード公開翌日に約 3 万件もの攻撃ログを観測

株式会社サイバーセキュリティクラウド(本社:東京都渋谷区、代表取締役:大野 暉、以下「サイバーセキュリティクラウド」)は、各業界の企業に対してサイバーセキュリティに関する注意喚起をリアルタイムに実施するため、自社独自に集約したサイバー攻撃に関するデータを分析した「サイバー攻撃速報」を発表いたします。

■Drupal の脆弱性について

Drupal はプログラム言語 PHP で記述されたオープンソースのモジュラー式フレームワークのコンテンツ管理システムです。

この度、Drupal 公式 Web サイトにおいて、Drupal 7.x および 8.x の複数のサブシステムにリモートコード実行の脆弱性(CVE-2018-7600(SA-CORE-2018-002))が存在すると公表されています。

Drupal 公式サイトお知らせ

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002

https://www.drupal.org/sa-core-2018-002

本脆弱性を悪用されると、当バージョンに該当する Drupal 利用ユーザーは、任意のコードが実行される可能性があります。

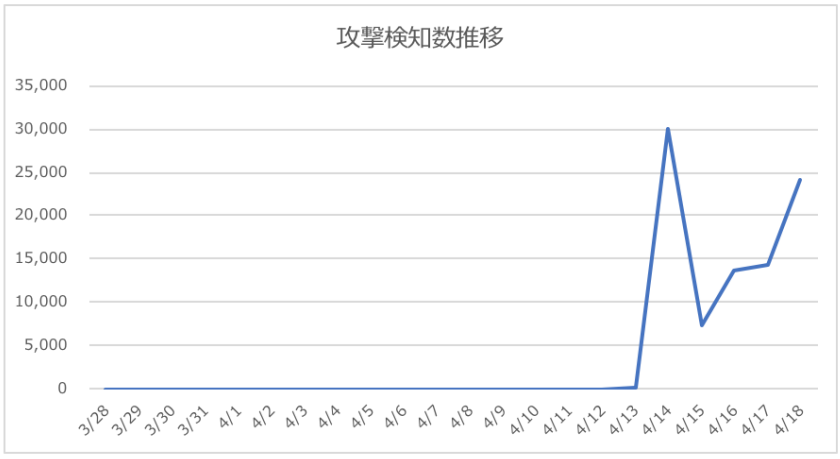
既に Drupal より最新バージョンが公開されており、7.x、8.5.x の利用ユーザーは、それぞれ Drupal 7.58、Drupal 8.5.1 へのアップグレードが推奨されています。

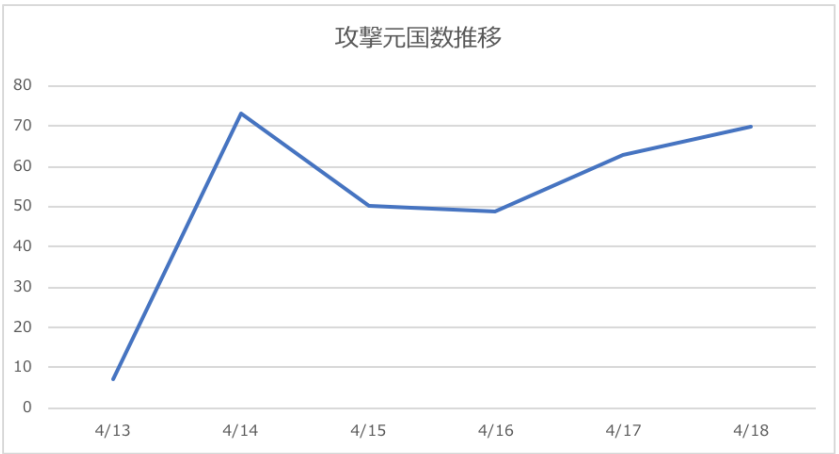
また、既にサポートが終了している 8.3.x、8.4.x に関しても、本脆弱性が深刻な内容であることから、それぞれ Drupal 8.3.9、Drupal 8.4.6 へのバージョンアップグレード、もしくは修正パッチの適用が推奨されています。

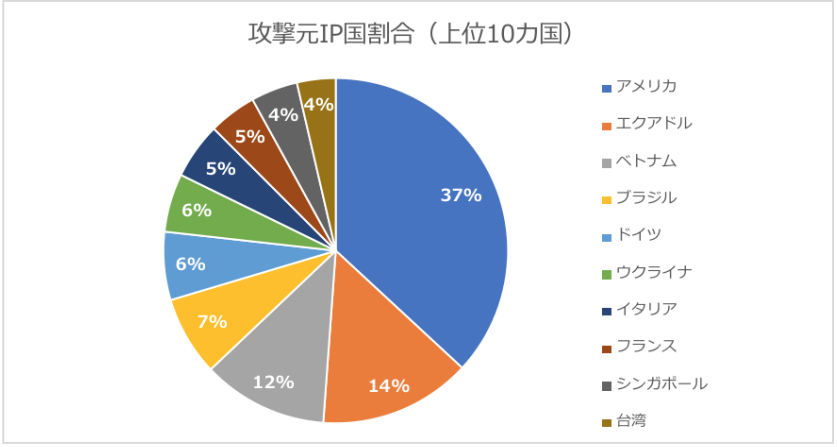
■Drupal 利用サーバーへの攻撃状況

この度、米国時間 4 月 12 日を起点に、複数のサイトで Drupal の脆弱性(CVE-2018-7600(SA-CORE-2018-002))を悪用する概念実証(PoC)コード公開されました。

これに伴い、当社が提供するクラウド型 WAF「攻撃遮断くん」をご利用中のユーザー様を対象に、本脆弱性を狙ったと思われる攻撃ログを集約し、分析・算出いたしました。







本脆弱性を悪用する攻撃は概念実証（PoC）コード公表から翌日に急増し、数日経過後も断続的に続いているため、脆弱性が発表された当初だけでなく、一定期間経過後でも注意が必要です。また、攻撃元 IP の国に着目した場合、攻撃元が分散されているため、ファイヤーウォールなどによる IP アドレスのブロックという運用対処は現実的には難しいことを示唆しています。
※攻撃元 IP の国は、あくまで攻撃に利用されている IP 元国の割合となり、攻撃者の実際の IP ではない可能性があります。

■クラウド型 WAF「攻撃遮断くん」の対応状況
なお、弊社にて提供するクラウド型 WAF「攻撃遮断くん」におきましては、本脆弱性を利用した攻撃に関して、検知し遮断するようシグネチャをアップデートしております。
しかし、Drupal をご利用のお客様においては、今後、深刻な脆弱性が発見されることもありますので、最新バージョンへのアップデートを強く推奨いたします。

「Drupal の脆弱性(CVE-2018-7600(SA-CORE-2018-002))を利用した攻撃に対応いたしました。」
https://www.shadan-kun.com/news/20180329-2/

■「攻撃遮断くん」について
「攻撃遮断くん」は、Web サイトへのサイバー攻撃を可視化・遮断するクラウド型 WAF の Web セキュリティサービスです。
官公庁や金融機関をはじめ、大企業からベンチャー企業まで業種や規模を問わず様々な企業にご利用いただき、
2013 年 12 月のサービス提供開始から約 3 年半で
累計導入社数・導入サイト数 国内第1位※1 を記録しています。

※攻撃遮断くんの名称、ロゴは、日本国における株式会社サイバーセキュリティクラウドの登録商標または商標です。
※1 出典:「クラウド型 WAF サービス」に関する市場調査（2017 年 8 月 25 日現在）＜ESP 総研調べ＞（2017 年 8 月調査）

■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 ： 〒150-0031 東京都渋谷区桜丘町 24-4 第 5 富士商事ビル 4 階

代 表 者 ： 代表取締役 大野 暉

設 立 ： 2010 年（平成 22 年）8 月

U R L ： 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」この理念を掲げ、サイバーセキュリティクラウドでは、自社で一貫して Web セキュリティサービスの開発・運用・保守・販売を行っています。

全ての企業様が安心安全に利用できるサービスを開発し、情報革命の推進に貢献するために私たちは挑戦し続けます。