Distributed via @police https://www.npa.go.jp/cyberpolice/

平成 30 年4月 18 日

Topic

Drupal の脆弱性（CVE-2018-7600）を標的としたアクセスの観測について

Drupal の脆弱性（CVE-2018-7600）を標的とするアクセスを観測しました。同ソフトウェアを利用している場合には、アップデートの実施等の適切な対策を早急に実施することを推奨します。

1 Drupal の脆弱性（CVE-2018-7600）について

Drupal は、オープンソースの CMS（コンテンツ管理システム）です。

平成 30 年3月 28 日に、Drupal に存在する深刻な脆弱性（CVE-2018-7600）が開発元から公表[i]されました。開発元によると、当該脆弱性が悪用された場合、遠隔から攻撃者が任意のコードを実行できるとしています。これらの脆弱性については、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）からも日本語での情報が公開[ii]されています。また、4月には、海外の共有ウェブサービスにおいて PoC[iii]が公開されていることを確認しました。

2 Drupal の脆弱性（CVE-2018-7600）を標的としたアクセスの観測について

4月 14 日以降、警察庁のインターネット定点観測システムにおいて、当該脆弱性を標的としたアクセスを観測しました（図1）。

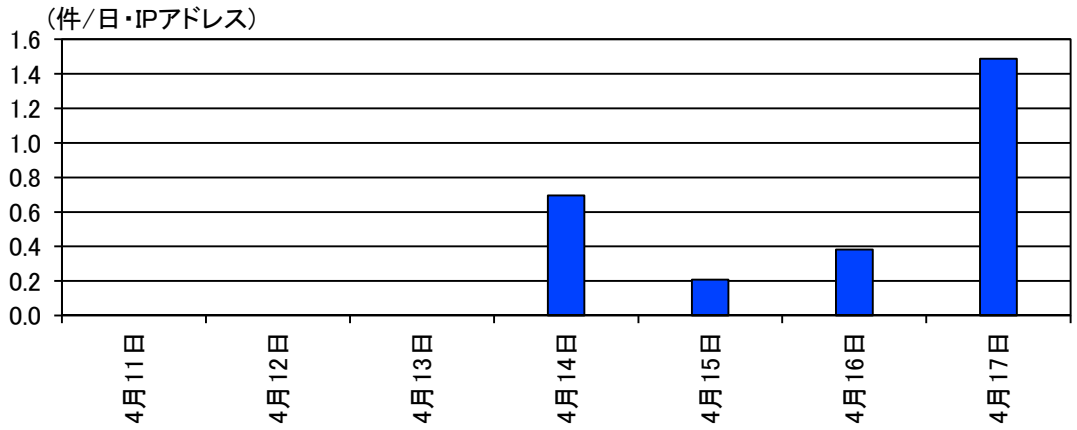

図1 Drupal の脆弱性（CVE-2018-7600）を標的としたアクセス件数の推移
（H30.4.11～4.17）

観測したアクセスは、前述した PoC に酷似した HTTP POST リクエストを送信するものでした。当該脆弱性が悪用可能であるかを探索するものだけでなく、外部サーバから不正プログラムの

[i] 「Drupal core – Highly critical – Remote Code Execution – SA-CORE-2018-002」
https://www.drupal.org/sa-core-2018-002

[ii] 「Drupal の脆弱性（CVE-2018-7600）に関する注意喚起」
https://www.jpcert.or.jp/at/2018/at180012.html

[iii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

ダウンロード及び実行を試みるものも確認しました（図2）。

図2　観測したアクセスのリクエスト内容（一部マスキングを実施）

3　推奨する対策

Drupal の利用者は、バージョンの確認を実施してください。脆弱性のあるバージョンは、以下のとおりです。

- Drupal 8.5.1 より前のバージョン
- Drupal 7.58 より前のバージョン

使用している Drupal が影響を受けることが判明した場合には、開発元から公開されている以下の対策済みバージョンへアップデートを実施してください。

- Drupal 8.5.1
- Drupal 7.58
- Drupal 8.4.6（サポート対象外）
- Drupal 8.3.9（サポート対象外）

脆弱性のあるバージョンを使用している場合は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル及び通信等が存在しないか確認してください。