2018 年 5 月 21 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：Drupal の脆弱性を狙った攻撃について

1. 概要

最近の仮想通貨市場の盛り上がりを反映して、サイバー攻撃においても、システムの脆弱性を悪用し仮想通貨を不正に取得しようとするケースが増加しています。

今回取り上げるのはオープンソースの CMS(コンテンツマネジメントシステム)である Drupal で発見された脆弱性です。この脆弱性に関しても、仮想通貨のマイニングを目的とした攻撃が世界中で多数報告されています。

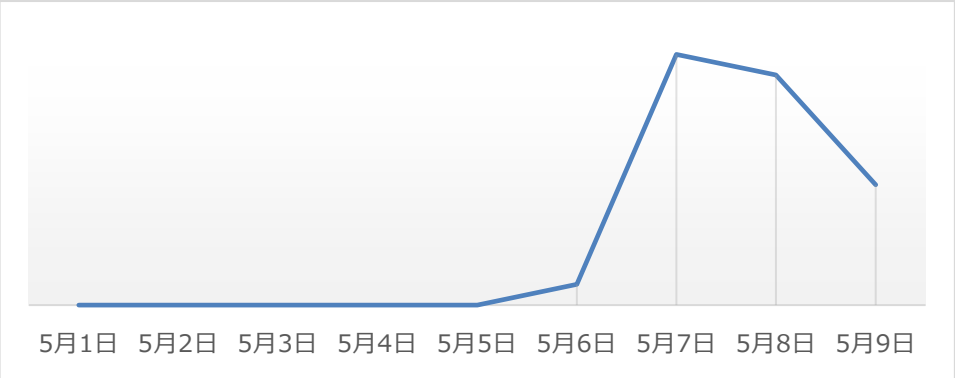
Drupal は WordPress や Joomla!に次いで普及している CMS です。企業の Web サイトでフレームワークとして利用されていることも多く、サイト管理者が Drupal を使用していることに気づいていないケースも考えられるため、注意が必要です。

2. 背景と現在の状況

2018 年 3 月 28 日に脆弱性 CVE-2018-7600 が公開され、続いて 4 月 25 日に CVE-2018-7602 が公開されました。いずれも、脆弱性のあるバージョンの Drupal が動作している Web サーバに対して、悪意を持った攻撃者が細工した HTTP リクエストを送ることで、サーバ実行ユーザ権限で任意のコードを実行することが可能となる RCE (Remote Code Execution)の脆弱性です。これらの脆弱性の重大度は、Drupal の開発元によって「Highly Critical」と設定されており、実際に攻撃による被害も報告されているため、早急に対策を実施する必要があります。

e-Gate センターにおいても、CVE-2018-7600 を狙ったと思われる通信を観測しています(図 1)。5 月に入ってからも継続的に攻撃活動が観測されているため、依然として警戒が必要です。

なお、CVE-2018-7602 を狙った攻撃は現在のところ確認されていません。一定の権限を有したユーザの認証情報を取得していることが攻撃の前提条件となるためと推測されます。ただし、ユーザ認証を要しない攻撃可能箇所が発見されることで、今後攻撃活動が活発となる可能性があります。

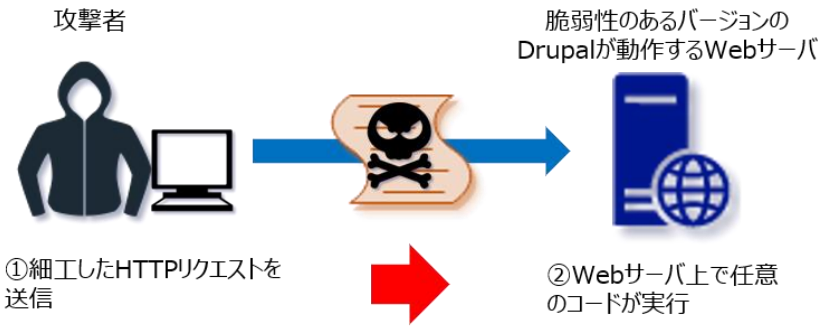


【図 1　CVE-2018-7600 を狙ったと見られる通信の推移】

3. 攻撃と対策

⑴ Drupal の脆弱性を突いた攻撃

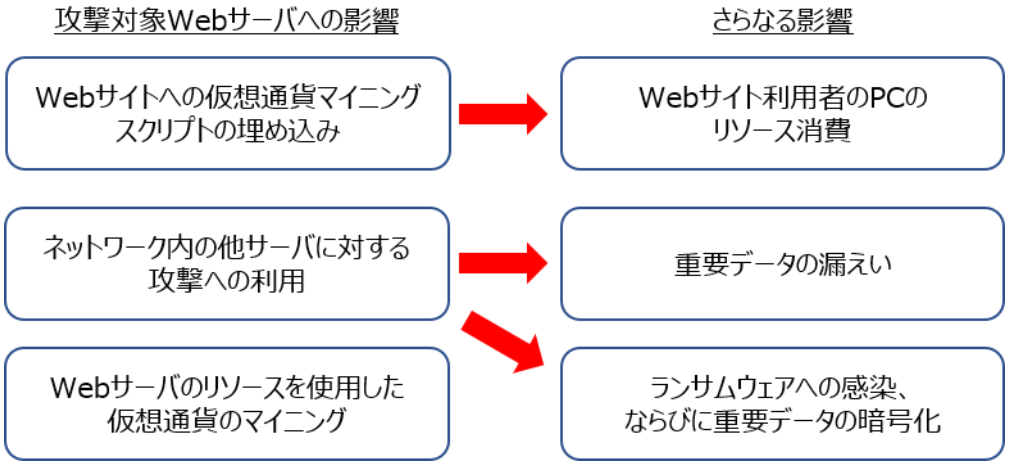
脆弱性のあるバージョンの Drupal では、一部のパラメータにおいてユーザの入力した値に対する検証が十分になされていません。攻撃者はそれを利用し、脆弱性のあるバージョンの Drupal が動作する Web サーバに対して細工を施した HTTP リクエストを送信することで、サーバ上で攻撃者が用意した任意のコードを実行します。



【図 2 攻撃イメージ】

⑵ 想定される影響

本脆弱性が悪用されることによる影響の例として、以下が挙げられます。



【図 3 影響の一例】

本脆弱性は攻撃者に任意のコードの実行を可能とするものですので、この他にも様々な被害を及ぼす可能性があります。ご使用の Web サーバ上で攻撃コードが実行されることで、直接被害を受けるだけでなく他のユーザに対して攻撃を行う側となってしまうおそれもあるため、ご注意ください。

⑶ 対象

次のバージョンの Drupal が本脆弱性の影響を受けます。

① CVE-2018-7600

- 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

② CVE-2018-7602

- Drupal 8.5.3 より前のバージョン
- Drupal 7.59 より前のバージョン

※サポートが既に終了している Drupal 6 系や Drupal 8.4 系以前でも本脆弱性の影響を受けることが発表されています。詳細は開発元の情報をご確認ください。

⑷ 対策

次のバージョンの Drupal について、本脆弱性の修正済みバージョン・セキュリティパッチが提供されています。

- Drupal 8.5.x
- Drupal 7.x
- Drupal 8.4.x
- Drupal 8.3.x

脆弱性対象バージョンをご使用の場合は最新版へのアップデートの実施を推奨いたします。また、ただちにアップデートが実施できない場合は、セキュリティパッチの適用による回避策をご検討ください。上記に記載の無いバージョンの対応については、開発元の情報をご確認ください。

⑸ 参考情報

① CVE-2018-7600

JPCERT/CC 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

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002
https://www.drupal.org/sa-core-2018-002

② CVE-2018-7602

JPCERT/CC Drupal の脆弱性（CVE-2018-7602）に関する注意喚起
http://www.jpcert.or.jp/at/2018/at180019.html

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-004
https://www.drupal.org/sa-core-2018-004

4. e-Gate の活用について

今回の攻撃はシステムの脆弱性を突く攻撃の 1 例です。ターゲットとなるサーバへの攻撃を早期に発見する為には、日々の運用監視が重要です。SSK の総合セキュリティサービス「e-Gate」のセキュリティ運用監視サービスをご活用頂くことで、精度の高い検知、早期発見による迅速な事後対応が可能となります。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp