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

令和２年 11 月 20 日

レポート

Wordpress 用 FileManager を標的としたアクセスの観測等について

- Wordpress 用 FileManager を標的としたアクセスの観測
- DockerAPI を標的としたアクセスの増加

1 Wordpress 用 FileManager を標的としたアクセスの観測について

Wordpress はウェブサイトを構築・管理するコンテンツマネジメントシステム(CMS)の1つであり、プラグインにより機能を追加することができます。令和2年9月１日に Wordpress 用 FileManager プラグインが更新[i]され、脆弱性が明らかになりました。この情報については、JPCERT/CC からも日本語での情報[ii]が公開されています。また、海外の共有ウェブサービスにおいて、当該脆弱性を対象とした PoC[iii]が公開されていることを確認しました。

警察庁のインターネット定点観測においては、9月 10 日及び 11 日に FileManager プラグインへのアクセスを観測し、10 月 13 日から当該アクセスの増加を観測しました。（図1）

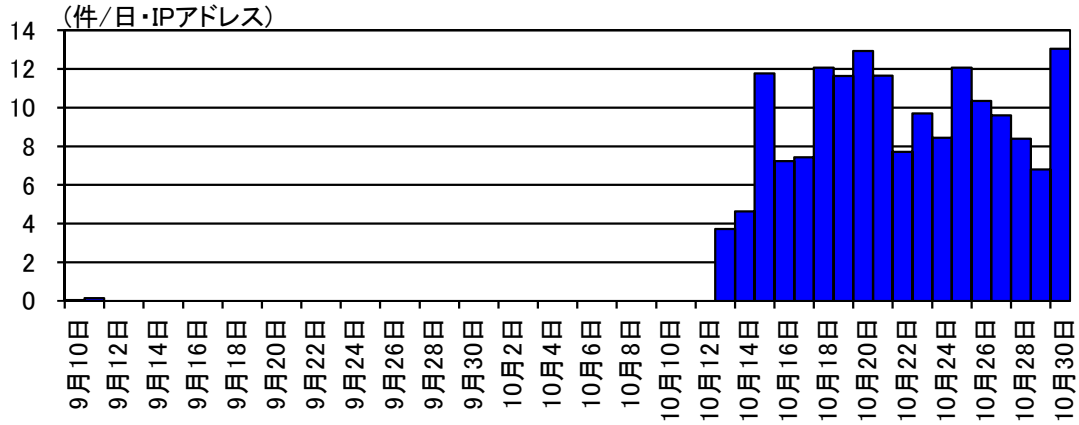

図１ 宛先ポート 80/TCP に対する WordPress 用 FileManager に対するアクセス件数の推移
（R2.9.10～R2.10.31）

[i] https://wordpress.org/plugins/wp-file-manager/

[ii] WordPress 用プラグイン FileManager の脆弱性について
https://www.jpcert.or.jp/newsflash/2020090301.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

観測したアクセスは、FileManager プラグインの説明書の取得を試みるものがほとんどであり、当該行為によってプラグインのバージョンを確認していると考えられます(図2)。

```
GET /wp-content/plugins/wp-file-manager/readme.txt HTTP/1.1
```

図2　WordPress 用 FileManager の説明書を取得するアクセスの例

また、少数ですが当該脆弱性を使用するアクセスも観測しました。

```
POST /wp-content/plugins/wp-file-manager/lib/php/[redacted].php HTTP/1.1
```

図3　WordPress 用 FileManager の脆弱性に対するアクセスの例
（一部マスキングを実施）

当該プラグインを悪用すると、第三者が任意のファイルをアップロードし、実行できるようになります。そのため、ウェブサーバの改ざん、ファイル蔵置及び情報漏えいの原因となります。

このため、Wordpress 用 FileManager の使用者は、バージョン 6.9 以降であることを確認してください。脆弱性のあるバージョンを使用している場合は、以下の対策を実施することを推奨します。

- 公開されている更新プログラムを適用し、ソフトウェアを最新の状態にしてください。
- Wordpress とプラグインを最新バージョンにアップデートしてください。

Wordpress を使用しており、脆弱性のあるプラグインを使用している場合、すで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、不審なイメージ、ファイル、プロセス、通信等がないか確認してください。

また、ウェブサーバが改ざんされた際、改ざんの原因となった脆弱性を修正することなく復旧した場合、同一の方法で再度改ざんされる可能性があります。ウェブページ復旧時には改ざんの原因となった脆弱性を修正してから公開を再開する必要があります。

当該プラグイン以外にも、Wordpress 及び各種プラグインには過去に脆弱性が公表されています。Wordpress を使用しているウェブページの管理者は、以下の対策を実施することを推奨します。

- Wordpress 及び各種プラグインに対して公開されている更新プログラムを適用し、ソフトウェアをアップデートしてください。
- 設定を確認し、不要な権限がないか確認してください。
- 必要のないプラグインを見直し、不要なプラグインは削除してください。
- 複雑で推測できないパスワードの使用、使用していないアカウントの削除等、アカウント管理を適切に行ってください。
- ウェブサイトに外見上変化のない改ざんが行われることがあります。不審なコンテンツの有無を確認してください。

2 DockerAPIを標的とした探索行為・情報取得行為の増加について

Docker はコンテナ型仮想実行環境の管理ソフトウェアであり、遠隔からネットワーク経由での操作も可能となる API が提供されています。設定を変更することにより、任意の TCP ポートで待ち受けを行い、ネットワーク経由での操作を行うことが可能です。

警察庁のインターネット定点観測においては、令和元年 11 月上旬から DockerAPI の探索行為の増加を観測し、令和元年 12 月 25 日に@police の Web サイトにおいて注意喚起[i]を行いましたが、令和2年9月以降、DockerAPI に対するアクセスの増加を観測しました(図4)。なお、令和2年 11 月にセキュリティベンダーより、「露出したDockerサーバ」についての注意喚起[ii]が公表されました。

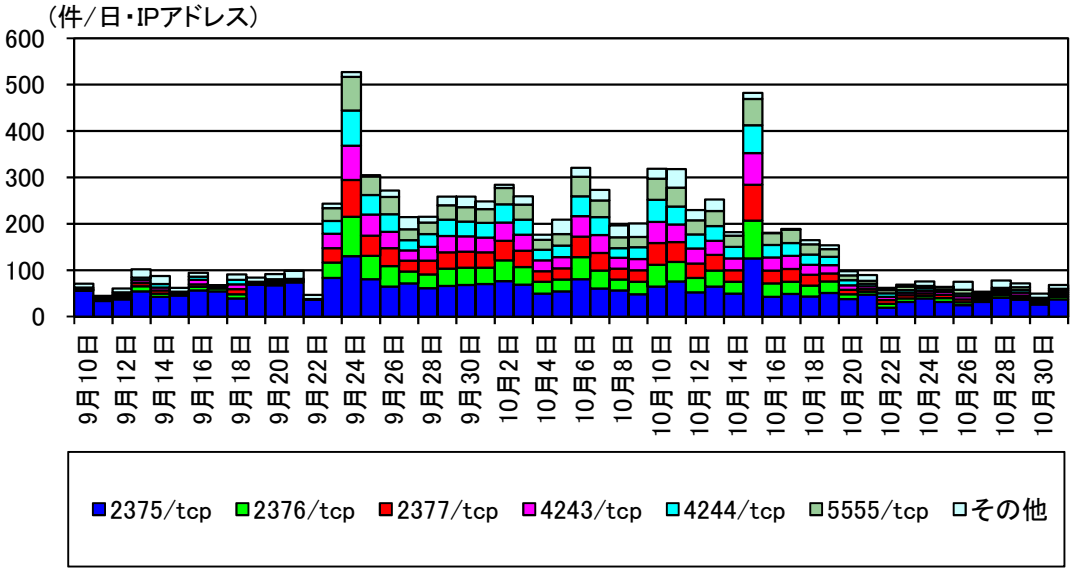

図4 DockerAPI に対するアクセス件数の推移(R2.9.10～R2.10.31)

観測されたアクセスは、Docker API を用いて、Docker のバージョン情報をリクエストするものがほとんどですが、稼動しているサーバの情報及びコンテナやコンテナイメージの情報をリクエストするアクセスも観測しました。これらの行為は、外部から操作可能な DockerAPI を探索する目的があると考えられます。DockerAPI に対するアクセス(表1)は、宛先ポート 2375/TCP、2376/TCP、2377/TCP、4243/TCP、4244/TCP、5555/TCP、2379/TCP 等で観測されています。

[i] DockerAPI を標的とした探索行為の増加について
https://www.npa.go.jp/cyberpolice/important/2019/201912251.html

[ii] 「露出した Docker サーバを狙い、不正マイニングと DDos の踏み台に悪用する攻撃が続発」
https://blog.trendmicro.co.jp/archives/26532

表1　観測した DockerAPI に対するアクセス

アクセス例
GET /v1.16/version
GET /version
GET /_ping
HEAD /_ping
GET /v1.18/coutainers/json
GET /v1.40/containers/json?all=1
GET /info
GET /images/json?

外部から DockerAPI が認証なしで利用できる場合、攻撃者が API を使用して、悪意のある Docker イメージを不正に作成、あるいは Docker イメージを使用し、ホストマシンへの侵入、攻撃の踏み台として悪用、暗号資産の採掘等を行う危険性も考えられます。

このため、DockerAPI を使用している場合は、以下の対策を実施することを推奨します。

- 必要がない場合は、外部から DockerAPI にアクセスできるように設定されていないか確認してください。
- 外部から DockerAPI へのアクセスを行う必要がある場合は、電子証明書による認証を行ってください。また、必要な送信元 IP アドレスのみに許可する、VPN を用いて接続することを検討してください。
- 公開されている修正プログラムを適用し、ソフトウェアを最新の状態にしてください。

外部から DockerAPI が認証なしで使用できる場合は、すで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、不審なイメージ、ファイル、プロセス、通信等がないか確認してください。