ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●「Movable Type」にサーバー乗っ取りの脆弱性、既に悪用も…IPA等注意喚起

https://scan.netsecurity.ne.jp/article/2021/11/09/46602.html
https://www.ipa.go.jp/security/ciadr/vul/20211020-jvn.html
https://www.jpcert.or.jp/at/2021/at210047.html
https://www.sixapart.jp/movabletype/news/2021/10/20-1100.html

このニュースをザックリ言うと･･･

- 11月5日(日本時間)、IPAとJPCERT/CCより、CMS(コンテンツ管理)ソフトウェア「Movable Type(以下MT)」の脆弱性(CVE-2021-20837)を悪用した攻撃について注意喚起が出されています。

- 脆弱性はMTのXMLRPC APIに存在し、サーバー上で任意のOSコマンドの実行が可能となるもので、10月20日に脆弱性に関する最初の注意喚起を発表していました。

- MT開発元のシックスアパート社からは既にセキュリティアップデート(Movable Type 7 r.5003 / Movable Type 6.8.3等)がリリースされている他、見知らぬPHPファイル等の設置やhtaccessファイルの書き換えといった攻撃の例が挙げられており、早急にアップデートの適用、または回避策としてXMLRPC APIへのアクセス制限を行うよう呼び掛けられています。

- なお、MTがベースのCMS「PowerCMS」も同じ脆弱性の影響を受けるとされ、同じくセキュリティアップデートが提供されています。

AUS便りからの所感等

- XMLRPC APIは外部ツールからコンテンツ編集を行う等で提供されていましたが、Movable Type 7では非推奨とされている模様です。

- MTと同じCMSであるWordPressでもXMLRPC APIが提供されているものの、DoS攻撃等を受ける可能性が指摘され、無効化する方法が多くのブログで紹介されています。

- Webサーバー以外のサーバーにおいても、使用しないあるいは第三者にアクセスされるべきでないポート等をフィルタリングする設定はセキュリティの確保において鉄則であり、使用しない機能が有効になっていないか、自前で、あるいは第三者機関の診断を受けてチェックを行い、適宜無効化することが肝要です。

- その他、多機能なソフトウェアには特に頻繁な脆弱性の報告とアップデートのリリースが付き物であると心得、速やかにアップデートを行う体制を用意した上で、サーバー上あるいはUTMにおいて不正なアクセスを遮断するWAF機能等の導入も検討することを推奨致します。


ScanNetSecurity

2021.11.9 Tue 8:00

「Movable Type」のXMLRPC APIにOSコマンド・インジェクションの脆弱性、悪用した攻撃も確認

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は11月5日、「Movable Type」のXMLRPC APIにおけるOSコマンド・インジェクションの脆弱性について発表した。影響を受けるシステムは以下の通り。

シェア　ツイート　送る

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は11月5日、「Movable Type」のXMLRPC APIにおけるOSコマンド・インジェクションの脆弱性について発表した。影響を受けるシステムは以下の通り。

Movable Type 7 r.5002 およびそれ以前 (Movable Type 7系)
Movable Type 6.8.2 およびそれ以前 (Movable Type 6系)
Movable Type Advanced 7 r.5002 およびそれ以前 (Movable Type Advanced 7系)
Movable Type Advanced 6.8.2 およびそれ以前 (Movable Type Advanced 6系)
Movable Type Premium 1.46 およびそれ以前
Movable Type Premium Advanced 1.46 およびそれ以前

シックス・アパート株式会社が提供するコンテンツ管理システム「Movable Type」のXMLRPC APIには、OSコマンド・インジェクションの脆弱性が存在し、遠隔の第三者によって任意のOSコマンドを実行される可能性がある。

JPCERT/CCでは11月5日現在、本脆弱性を実証するコード（PoC）が公開され、10月27日から脆弱性の有無を調べる通信が、11月1日には脆弱な環境に不審ファイルを配置することを目的とした通信を株式会社ラックで観測しており、実際にファイルが配置される事例も確認している。

●オンラインゲームのチートツール等からマルウェア「RedLine」に感染する恐れ

https://www3.nhk.or.jp/news/html/20211108/k10013338171000.html
https://security.srad.jp/story/21/11/10/1619240/

このニュースをザックリ言うと･･･

- 11月8日(日本時間)、NHKのニュースにて、「感染経路の7割余りが、不正なソフトウエアのインストールが原因とみられる」とされるマルウェア「RedLine Stealer(以下RedLine)」について報じられています。

- RedLineは感染したPCからクレジットカード情報やECサイトのパスワードを奪取するとされ、都内セキュリティ企業アルモリス社が国内の感染例約920件を調査した結果、41%がオンラインゲームのチートツール(不正等を行う)から、31%がクラックウェア(有料のソフトを無料で使えるようにする)からの感染だったとのことです。

- 一方で、PCの画面に表示されるポップアップのクリックによる感染は2%程度とされ、RedLineへの感染の大半は自ら不正なソフトを使うことによるものだったと結論付けられており、同社では「無料だからとのせられず、ソフトは公式サイトからインストールする」ように呼び掛けています。

AUS便りからの所感

- RedLine自体は2020年3月頃から存在が報告されており、分散コンピューティングで新型コロナウイルスの解析等を行うプロジェクトを騙る等、今日まで様々な手口で拡散している模様です。

- 開発を自動化するツールMSBuildを悪用し、RedLineがPCのディスク上にファイルを残さないいわゆる「ファイルレスマルウェア」として拡散したケースもあり、その際にはアンチウイルスでの検出が困難だったとの報告もあります。

- あくまでマルウェアの種類によって主に利用する感染経路が異なるということであり、マルウェア全体の傾向を示すものでこそありませんが、不正行為を行おうとするユーザーを誘導してマルウェア感染に誘導する手口は今後も他のマルウェアに利用されることが考えられ、アンチウイルスやUTMで防御を固めることはもちろん、マルウェア感染以外にも様々なリスクを孕んでいる不正行為には手を出さず、ソフトウェアを正規の手順で購入する等もまた、自衛策として重要と言えます。

●「メールプラン、セキュリティ強化第2弾リリースのお知らせ」…ばらまきメールとフィッシングサイトに注意喚起

https://xtech.nikkei.com/atcl/nxt/news/18/11647/

このニュースをザックリ言うと･･･

- 11月11日(日本時間)、日経クロステックにて、メールアカウント情報を詐取しようとするばらまきメールとフィッシングサイトについて取り上げられています。

- 記事によれば、メールの件名は「メールプラン、セキュリティ強化第2弾リリースのお知らせ」等で、リンクをクリックすると、Webメールのログイン画面に偽装しメールアドレスとパスワードを奪取するフィッシングサイトが表示されるとのことです。

- セキュリティ技術者有志による「ばらまきメール回収の会」によれば、正規のWebサイトの改ざんによって作成されたフィッシングサイトが1日に複数件確認され、11月以降、同11日時点で1000件、1日に100件以上のペースでアカウントの奪取が発生しているとのことです。

AUS便りからの所感

- フィッシングサイトのログイン画面は、今日大手のWebメールサービスでは使われることが少ない古いデザインではありますが、ISPや組織が提供するWebメール次第では騙される可能性は皆無とは言えず、普段利用する各種サービスについてはブラウザーのブックマークに登録し、そこからアクセスするよう心掛けるようにし、適宜メールのリンク先とブックマークからアクセスするログイン画面とのURLを比較すること等が、自衛策として有用です。

- 前述した「ばらまきメール回収の会」も推奨するとおり、メールの件名で検索し、フィッシング対策協議会のような団体からの注意喚起やSNS等での報告がないか確認するといった慎重な行動をとること、その他にもメーラーやブラウザーのアンチフィッシング機能等があれば必ず有効にすることが、フィッシングメールの脅威から回避するために大切です。