— AUS（アルテミス・ユーザ・サポート）便り 2016/05/16号 —
http://www.artemis-jp.com

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。

●ソフトウェア脆弱性を突いた個人情報流出･･･エイベックスから35万件、栄光ゼミナールから2761件

http://www.sankei.com/affairs/news/160429/afr1604290041-n1.html
http://news.livedoor.com/article/detail/11494979/

このニュースをザックリ言うと･･･

- 4月28日（日本時間）、大手音楽会社のエイベックス・グループ・ホールディングス社は、同社アーティストの公式サイトが不正アクセスを受け、キャンペーン応募者などの個人情報約35万件が流出した恐れがあると発表しました。

- 流出したとされる個人情報は、名前・住所・メールアドレス・電話番号等で、クレジットカード番号等は含まれていないとのことであり、アクセスログの解析により、サイトで使用しているソフトウェアの脆弱性を突いた不正アクセスがあったことが判明した模様です。

- 同29日には、学習塾大手の栄光ゼミナールがやはりサイトで使用しているソフトウェアの脆弱性を突かれ、学校別説明会に申し込んだ生徒と保護者の個人情報計2761件が流出したことが発表されています。

AUS便りからの所感等

- 4月21日・22日に相次いで発表（AUS便り2016/05/02号参照）された一連の個人情報流出とは「OSコマンドインジェクション」の脆弱性を突いたものである点が共通しており、特に一部報道や栄光ゼミナールの発表から、「ケータイキット for MovableType」（http://www.keitaikit.jp/）の脆弱性を突かれたとみられています。

- MovableTypeによってサイトを構築、かつ携帯電話向けサイトの提供のために当該ソフトウェアを用いている場合は、必ずアップデートを行ってください。

- 一部前回の記事で述べたことの繰り返しとなりますが、不正アクセスの早期発見のためにも、UTMの設置等による対応を強く推奨します。

産経ニュース

エイベックスで個人情報35万件流出か　公式サイトに不正アクセス

ツイート　反応　おすすめ 26　G+1 0

多数の人気アーティストを抱える音楽会社「エイベックス・グループ・ホールディングス」は、アーティスト公式サイトに不正アクセスがあり、キャンペーンに応募した人のデータなど、個人情報約35万件が流出した可能性があることを明らかにした。

同社の発表によると、流出した恐れがあるのは名前や住所、メールアドレス、電話番号など。同社がアクセスログ（記録）を解析したところ、サイトで使用しているソフトウエアの脆弱（ぜいじゃく）性を突いた不正アクセスがあったことが判明したという。

同社は対策本部を設置し、脆弱性に関する対策を実施した。不正アクセスの内容の分析を行い、セキュリティー強化を進めていくとしており、「差出人や件名にエイベックスや所属アーティストの名前が書かれた不審なメールやメッセージなどが届いた場合は、開封や応答を控えてほしい」と呼びかけている。

不正アクセスによる個人情報の流出をめぐっては、日本テレビが21日、同社ホームページ（HP）が不正アクセスを受け、最大約43万件の個人情報が流出した可能性があると発表した。22日にはFMラジオ局「J-WAVE」が同社HPに不正アクセスがあり、リスナーの個人情報約64万件が流出した可能性があると発表した。

livedoor NEWS

「栄光ゼミナール」サイトに不正アクセス、個人情報2761人分流出

2016年5月7日 15時30分　スポーツ報知

学習塾大手「栄光ゼミナール」は7日までに、同社のサイトが不正アクセスされ、生徒や保護者計2761人分の個人情報が流出したと発表した。

栄光ゼミナールによると、流出した個人情報は名前や電話番号、メールアドレス、学校名など。2007年5月7日～7月16日の間に、同社サイト上から学校別説明会を申し込んだ個人情報だという。

今年4月21日に、同社サイトで使用していたソフトウェアのメーカーが公開した修正ファイルを適用した後、アクセスログを解析したところ、情報流出が判明。原因となったソフトウェアを削除するとともに、流出した個人情報のデータをサーバー上から削除し、安全な場所に保管した。

栄光ゼミナールは4月29日付でサイト上に事実関係の説明と謝罪文を掲載。今後は情報管理を徹底するとともに、不審なメールや電話への注意喚起を呼びかけている。

●画像処理ツール「ImageMagick」に脆弱性、広い範囲に影響の恐れ

http://www.itmedia.co.jp/enterprise/articles/1605/06/news047.html

このニュースをザックリ言うと･･･

- 5月3日頃（米国時間）、画像処理ツール「ImageMagick」に深刻な脆弱性「ImageTragick」が存在することが開発者や脆弱性の発見者、および米CERT/CC等から発表されました。

- 脆弱性は複数報告されており、攻撃者が細工した画像データをImageMagickで処理することにより、サーバ上で任意のコードが実行され、サーバ上のファイルが不正に読み書きされる、あるいはサーバが乗っ取られるといった可能性があるとされています。

- 脆弱性の一部については新しいバージョンで修正されており、その他の脆弱性についても回避策が提示されています。


ITmedia エンタープライズ

2016年05月06日 08時04分 更新

画像処理ツール「ImageMagick」に脆弱性、広い範囲に影響の恐れ

PHP、Ruby、NodeJS、Pythonなど多数のプログラミング言語にも使われているImageMagickに脆弱性が見つかった。

[鈴木重子, ITmedia]

PHP、Ruby、NodeJS、Pythonなどの主要プログラミング言語でも使われている画像処理ツール「ImageMagick」に深刻な脆弱性が見つかった。影響が広範に及ぶことや、脆弱性を突く攻撃の発生が伝えられていることなどから、米セキュリティ機関US-CERTなどはパッチの適用を急ぐよう呼び掛けている。

脆弱性問題をイメージしたアイコン画像（解説サイトより）

この問題は通称「ImageTragick」とも呼ばれている。解説サイトやセキュリティ機関のCERT/CCによると、ユーザーの入力内容がImageMagickで適切に検証されないまま処理されてしまうことが原因で、ユーザーがアップロードした画像を使って攻撃コードを実行される恐れがある。

この脆弱性はRed Hat、SUSE Linux、Ubuntuなど主要Linuxディストリビューションで影響が確認されているほか、PHPの「imagick」、Rubyの「rmagick」「paperclip」、NodeJSの「imagemagick」など、ImageMagickを使ったライブラリ多数が影響を受けるという。

AUS便りからの所感等

- ImageMagickは主にLinux上で動作し（Windows版も存在）、PHP・Ruby・NodeJS・Pythonといった各種プログラミング言語からも使用されており、例えば、Webアプリケーションにおいて、アップロードされた画像の変換を行うために用いている等のケースで注意が必要です。

- 最新バージョンへのアップデートだけでは全ての脆弱性の対策はできず、「policy.xml」という設定ファイルの修正が必要になる模様で、一部Linuxディストリビューションではこれらの両方を行うものもあるようですが、ベンダー等からの情報を十分に精査し、必要な対策が全て行われているか確認すべきでしょう。

- 不正な画像ファイルを送信して脆弱性を突こうとする攻撃に対しては、UTMの設置によってもある程度は回避することが可能とみられますが、やはり最終的には上記の対策を一通りとることが求められます。

●TFTPとSQL Serverの探索、3月に急増･･･警察庁発表

http://www.npa.go.jp/cyberpolice/topics/?seq=18319

このニュースをザックリ言うと･･･

- 4月28日（日本時間）、警察庁が3月期のインターネット観測結果等を発表し、TFTPサービスとMicrosoft SQL Serverを探索していると考えられるアクセスが急増したとして警告しています。

- TFTPで用いられるUDPポート69番へのアクセスは3月9日以降急増し、最大で4.5件/日・IPアドレス（3月11日）を記録しており、また、当該サービスを悪用することにより、攻撃パケットが約60倍に増幅するとされるリフレクター攻撃について警告する論文が3月上旬に発表されたことも取り上げられています。

- 一方で、SQL Serverで用いられるTCPポート1434番へのアクセスも3月14日以降急増、最大で1200件/日・IPアドレス（3月17日）を記録しており、その多くはSQL Serverの情報を取得するためのアクセスだったとされており、この他、管理者アカウントへパスワードなしでログインしようとするアクセスについても、今回の急増前から確認されています。


@police

平成 28 年 4 月 28 日

インターネット観測結果等

（平成 28 年3月期）

- 宛先ポート 69/UDP に対するアクセスの増加
- Microsoft SQL Server を探索するアクセスの増加

1 宛先ポート 69/UDP に対するアクセスの増加

定点観測システムでは、3月 10 日以降、69/UDP を宛先ポートとするアクセスの増加を観測しました（図1）。69/UDP は、簡易なファイル転送を行うための通信プロトコルである TFTP において使用されるポートです。

図1 宛先ポート 69/UDP に対するアクセス件数の推移

AUS便りからの所感等

- TFTPはネットワーク機器の設定の保存・読み込みで用いられる場合がありますが、認証機能等を持っていない簡素なプロトコルであり、内部ネットワーク上で用いられることを想定しているため、インターネット上の不特定多数からアクセスされるべきではありません。

- データベースサーバについても、通常はWebアプリケーション等からアクセスされるものであり、特に意図していない限り、第三者からの直接アクセスはやはり危険なものとなります。

- ともあれ、想定していない相手からアクセスされるべきでないサービスへの不正アクセスに対しては、適宜OSやUTM等によるフィルタリングは欠かせないでしょう。