— AUS（アルテミス・ユーザ・サポート）便り 2017/02/13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。

●WordPressに不正投稿を許す脆弱性、Web改ざん多発の原因か？

http://www.itmedia.co.jp/enterprise/articles/1702/09/news064.html
http://www.ipa.go.jp/security/ciadr/vul/20170206-wordpress.html

このニュースをザックリ言うと・・・

- 2月6日（日本時間）、情報処理推進機構（IPA）より、ブログツール「WordPress」に重大な脆弱性が発表されたとして注意喚起が出されました。

- 問題となる脆弱性はWordPress 4.7.0～4.7.1に存在するもので、外部からWordPressにログインすることなしに、不正な投稿・既存の投稿の改変を容易に行うことが可能なものとされており、1月26日にリリースされた4.7.2で修正され、2月1日に脆弱性の存在が公表されています。

- 脆弱性を発見した、WAFサービスやWordPress用セキュリティプラグイン等を提供するセキュリティベンダーの米Sucuri社によれば、脆弱性の公表から48時間足らずでこれを悪用する攻撃コードが出回り、また複数のハッキング集団によるWebサイトの改ざんも多く確認されているとして、至急WordPressのアップデートを行うよう呼び掛けています。

AUS便りからの所感等

- バージョン4.7.0で導入された「REST API」機能に存在する脆弱性であり、4.6系以前の場合は影響しませんが、特に自動更新を行っている場合は多くのケースで4.7.0以降となっているとみられ、外部からサイト改ざんに悪用される恐れがあります。

- Sucuri社の発表によれば、最も頻繁に活動しているとみられるハッキング集団によって改ざんされたページが2月6日の時点でGoogleの検索に66,000件もヒットしていたとのことで、その後も被害は拡大しているとみられ、2月9日現在ではヒット数が146,000件にまで拡大している模様です。

- WordPressを用いてWebサイトを構築している場合、最初にコンテンツを投稿したきり放置しているケースが最も危険と言え、WordPressを採用しているサイトの管理者は至急バージョンを確認し、4.7.0～4.7.1の場合はすぐ4.7.2以降へのアップデートを行った上で、投稿内容が改ざんされていないか確認することを強く推奨致します。

- この脆弱性については、『危険すぎる』という理由から修正バージョンのリリース後しばらくはSucuri社による公表が控えられていた一方で、公表までの間に同社はWAFサービスを提供する同業他社にも情報提供を行っていたという経緯があり、WAFによっては今回の脆弱性を突いた攻撃リクエストを遮断する設定が公表前に登録されたものもあったとのことです。

- WordPressの運営には、こういった業者が提供するWAFサービス、WordPress向けのセキュリティプラグイン、あるいはUTMをはじめとするアプライアンスのWAF機能による防御が必要不可欠となるでしょう。


ITmedia エンタープライズ

2017年02月09日 08時41分 更新

WordPressの脆弱性突く攻撃が激増、6万以上のWebサイトで改ざん被害

脆弱性情報が公開されてから48時間足らずの間に悪用コードが投稿され、脆弱性のあるサイトを探して攻撃を試す動きはインターネット全体に広がった。ハッキングされたWebサイトの数は6万6000以上にのぼり、現在も増え続けている。

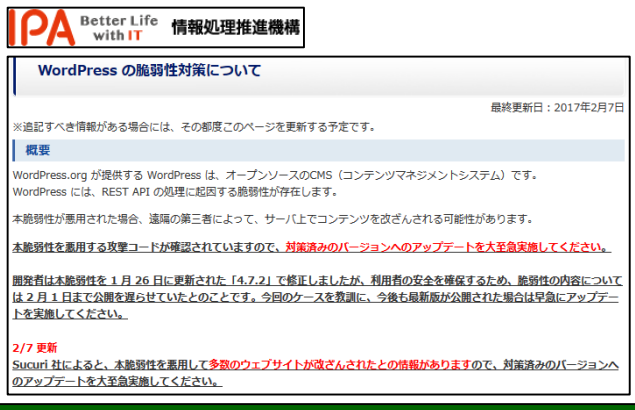
[鈴木聖子，ITmedia]

1月下旬のパッチで修正された、WordPressの深刻な脆弱性を突く攻撃が、わずか2週間足らずの間に激増し、多数のWebサイトの問題を発見したセキュリティ企業の

WordPressは1月26日に公開した更に深刻なWordPress REST APIの脆弱いた。この問題を悪用された場合、該ツやページを改ざんできてしまう可能

問題

「WordPress」では、細工したリクエストを送信することにより、投稿内容を改ざんすることが可能です。


IPA Better Life with IT 情報処理推進機構

WordPress の脆弱性対策について

最終更新日：2017年2月7日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

WordPress.org が提供する WordPress 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）です。
WordPress には、REST API の処理に起因する脆弱性が存在します。

本脆弱性が悪用された場合、遠隔の第三者によって、サーバ上でコンテンツを改ざんされる可能性があります。

本脆弱性を悪用する攻撃コードが確認されていますので、対策済みのバージョンへのアップデートを大至急実施してください。

開発者は本脆弱性を 1 月 26 日に更新された「4.7.2」で修正しましたが、利用者の安全を確保するため、脆弱性の内容については 2 月 1 日まで公開を遅らせていたとのことです。今回のケースを教訓に、今後も最新版が公開された場合は早急にアップデートを実施してください。

2/7 更新

Sucuri 社によると、本脆弱性を悪用して多数のウェブサイトが改ざんされたとの情報がありますので、対策済みのバージョンへのアップデートを大至急実施してください。

●牛角の偽キャンペーンがTwitterで出回る、公式が注意喚起

http://nlab.itmedia.co.jp/nl/articles/1702/05/news029.html

このニュースをザックリ言うと・・・

- 1月24日（日本時間）、焼肉レストランチェーン「牛角」等を運営するレインズインターナショナル社より、牛角をかたる偽キャンペーンがTwitterで出回っているとして注意喚起が出されました。

- 同社によれば、偽キャンペーンは「牛角 焼肉お食事代 5万円分プレゼント」等と称したスクラッチキャンペーンで、スクラッチを削ると必ず当選画面が表示され、プレゼント受け取りのためとして要求したメールアドレスに対してスパムメールが送信されるようになるというものです。

- 2月4日にも同様の偽キャンペーンの広告ツイートが表示されたとの報告が相次ぎ、牛角の公式Twitterアカウントで再び注意喚起が出されています。

AUS便りからの所感等

- 今回発覚したのは、広告を表示しただけでマルウェアに感染する類のものではない、比較的原始的なフィッシング詐欺ですが、Twitterの場合は不審なアプリとの連携を要求され、スパムツイートを投稿するといったケースもあります。

- SNSにおいてこういう広告に遭遇した場合は、それが不審なものでないか（アカウント名がランダムな文字列、URLがおかしい等）、あるいは他のユーザがどういう反応を示しているか検索等を行い、今回のような悪質な広告については、他のユーザへの被害拡大を抑えるため、可能な限り報告していくことを推奨致します。

- ブラウザやアンチウイルス・UTM等のアンチフィッシング機能により、詐欺サイトへのアクセスを食い止められる可能性もありますし、屋外等でスマートフォンからインターネットにアクセスする場合も、UTMへのVPN接続を経由してのアクセスにより、こういったセキュリティ機能による防御が期待できるでしょう。

●2016年は「日本におけるサイバー脅迫元年」

http://internet.watch.impress.co.jp/docs/news/1041564.html

このニュースをザックリ言うと・・・

- 1月10日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、2016年の日本国内でのサイバー犯罪動向に関するまとめが同社ブログ等で発表されました。

- 同社によれば、個人・法人ともに最大の脅威となったのは「ランサムウェア」で、2016年における同社製品でのランサムウェア検出台数は62400件（個人46700件・法人15700件）と、2015年における6700件（個人5700件・法人1000件）の実に9.3倍となっており、まさに『日本におけるサイバー脅迫元年』となったとしています。

- 一方で、同社が全世界で観測したランサムウェアによる2億6000万件の攻撃のうち、日本をターゲットにしたものは2%に留まり、まだ日本への攻撃は本格的ではないとしてはいるものの、10～11月にかけて、日本企業にターゲットを絞ったランサムウェア攻撃の兆候があったことを挙げ（AUS便り 2016/11/28号参照）、「メール・Webの2つの経路において侵入を検知するセキュリティ対策製品の導入」「ブラウザ・Flash・Java等のアップデートの実施」「定期的なデータのバックアップ」等を呼び掛けています。

AUS便りからの所感等

- ランサムウェアは昨年における最も有名なマルウェアの一つとなり、これに便乗した「偽のランサムウェアによる脅迫」についても先週取り上げています（AUS便り 2017/2/6号参照）。

- これまでの常識からの見直しが必要なものとこれまでの防御策が通用するもの、あるいは、感染自体を防御する視点と感染してしまったときの被害を最小限に抑える視点、それぞれの対策を確実に実行できるようシステムとネットワーク構成の点検を適宜行っていくことが重要となってきます。