WordPress におけるコンテンツインジェクションの脆弱性に関する調査レポート

【概要】
CMS(*1)ソフトウェアとして広く使われている WordPress に、コンテンツインジェクション可能な脆弱性の攻撃コードが発見されました。

この脆弱性は WordPress の投稿の取得や新規追加、更新を行うことができる REST API にて、リクエスト受信時におけるアクセス権確認処理の不具合があるために生じる脆弱性です。なお、REST API は、WordPress4.7.0 または 4.7.1 を使用するウェブサイトではデフォルトで有効になっています。
この脆弱性を利用した攻撃が成立した場合、ウェブサイトの投稿内容やページの内容を変更または削除される危険性があります。

本レポート作成（2017 年 2 月 3 日）時点において、開発元より脆弱性を修正したバージョンがリリースされております（2017 年 1 月 26 日付）。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性の再現性について検証を行いました。

*1CMS(Content Management System の略):ウェブサイトのページ作成において、技術的な知識がなくても容易にページを作成できるような仕組みを用意したシステム。

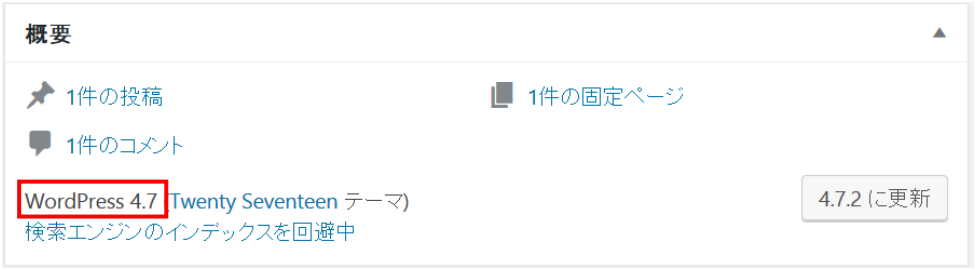
【影響を受ける可能性があるシステム】
- WordPress 4.7.0
- WordPress 4.7.1

【対策案】
開発元より、この脆弱性を修正するプログラムがリリースされています。
当該脆弱性の修正を含む最新のバージョンを適用していただくことを推奨いたします。

ただちに最新版へアップデートすることが困難な場合、REST API を無効化するプラグインをインストールすることで、攻撃を回避できる可能性があります。下記、弊社検証において、同プラグインをインストールすることで攻撃を回避できたことを確認しております。

【バージョン確認方法】

WordPress 管理画面のダッシュボード内、概要の項目より、WordPress のバージョンを確認できます。



【参考サイト】

Content Injection Vulnerability in WordPress

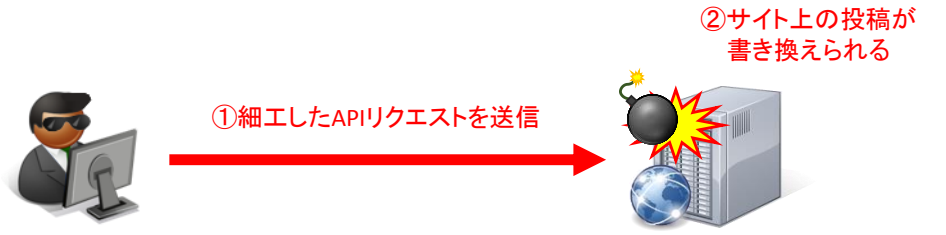
【検証概要】

ターゲットシステムに対し、細工した API リクエストを送信することにより、同システムの投稿内容が変更されることを確認します。これにより、攻撃者が投稿内容を任意の内容に書き換えられることを確認できます。

【検証ターゲットシステム】

CentOS 7.3 + WordPress 4.7.0

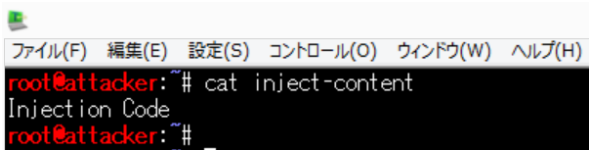
【検証イメージ】



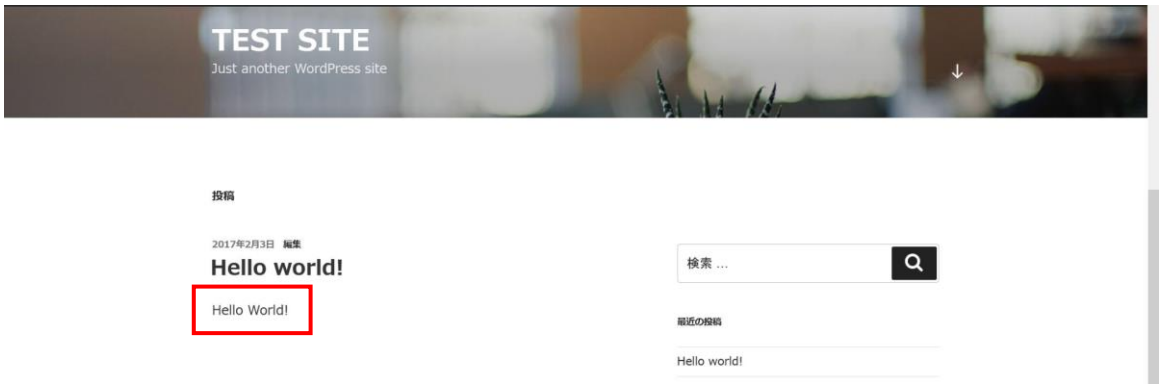
【検証結果】

任意の投稿内容[画像 1]を使用して攻撃コードを実行したところ、ターゲットシステムの投稿内容が変更されました。これにより、攻撃者はターゲットシステムの投稿内容を、任意の内容に書き換えることが可能であることが確認できました。

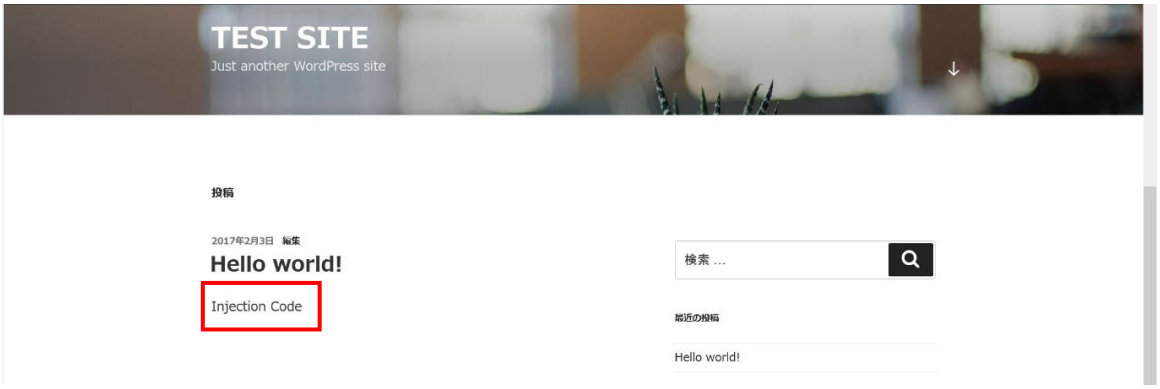
[画像 1]



[ターゲットシステムの投稿内容(攻撃コード実行前)]



[ターゲットシステムの投稿内容(攻撃コード実行後)]



【更新履歴】

2017 年 2 月 3 日 ： 初版公開