

BLOG

baserCMSプラグイン BurgerEditorの複数の脆弱性について

いつも BurgerEditor をご利用いただき、誠にありがとうございます。

この度、株式会社ディーゼロが提供するbaserCMS用プラグイン「BurgerEditor」において、複数の脆弱性が存在することが確認されました。 これらの脆弱性を修正した最新版を公開いたしましたので、対象バージョンをご利用中のお客様におかれましては、速やかに最新版へのアップデートをお願い申し上げます。

脆弱性の概要

以下の脆弱性に対応しております。

- アップロードするファイルの検証が不十分（CWE-434, CVE-2026-84063）
- ユーザ識別情報操作による権限チェック回避（CWE-639, CVE-2026-84062 ）

アップロードするファイルの検証が不十分 (CVE-2026-84063)

管理者向けに任意の拡張子を許可する設定（ `Bge.allowedAdmin` ）が有効な場合において、実行され得る拡張子のファイルを公開ディレクトリへ保存できてしまう状態でした。

これにより、当該製品にログイン可能な攻撃者によって、保存先URLへの未認証アクセスを通じて任意のPHPコードを実行される可能性があります。

ユーザ識別情報操作による権限チェック回避 (CVE-2026-84062)

当該製品にログイン可能な攻撃者によって、ページの内容を改ざんされる可能性があります。

影響を受けるバージョン

CVE-2026-84063 の影響を受けるバージョン

- BurgerEditor 3.2.0から3.4.0
- BurgerEditor 2.28.0から2.30.0

CVE-2026-84062 の影響を受けるバージョン

- BurgerEditor 3.0.0から3.4.0

修正内容

実行可能ファイルのアップロードを常に拒否

`Config/setting.php` にて `Bge.deniedExtension` の設定を追加し、`allowedAdmin` やシステム管理者権限にかかわらず、サーバーサイドで実行され得る拡張子を常に拒否するように変更しました。

なお、`Bge.allowedAdmin` 自体は廃止しておらず、デフォルト値も false のままです。
`allowedAdmin=true` の設定においても、`.psd` 等の入稿用途のファイルは従来通りご利用いただけます。

アップロードディレクトリの保護（.htaccessの自動設置）

アップロードディレクトリに `.htaccess` を設置し、保存済みファイルの実行および直接アクセスを遮断する仕組みを追加しました。

- `files/bgeditor/other/` ：dlアクション経由でのみ配信とするため、直接アクセスを全面拒否します。
- `files/bgeditor/img/` ：画像の直接配信が必要なため、実行系の拡張子に対するアクセスのみ拒否します。

※ この `.htaccess` はプログラムの初期化時およびアップロード処理の入口で自動生成されるため、既存の導入済みサイトにおきましても**再インストールなしで適用されます**。

対策方法

プラグインを最新版にアップデートしてください。

- BurgerEditor `v3.4.1`
- BurgerEditor `v2.30.1`

謝辞

本脆弱性は、野口晋義氏からIPAへご報告いただき、JPCERT/CCを通じて調整が行われました。

ご報告いただきました野口氏に深く御礼申し上げます。

今後とも BurgerEditor をよろしくお願い申し上げます。

2026/09/04

≪ baserCMSプラグイン BurgerEditorのディレクトリリスティングの脆弱性について（Vulnerability of Directory Listing in the baserCMS Plugin BurgerEditor） |

TOP

Copyright © 2014 D-ZERO Co.,Ltd. All Rights Reserved.