User Enumeration via Timing Side-Channel in Authentication Endpoint

Moderate **RARgames** published **GHSA-8mj9-p99h-jhxp** last week

Package

4gaBoards

Affected versions

3.3.4

Patched versions

3.3.5

Description

Summary

4ga Boards v3.3.4 and earlier is vulnerable to user enumeration via a timing side-channel in the login endpoint (`POST /api/access-tokens`). When an invalid username/email is provided, the server responds immediately (~17ms average). When a valid username/email is provided with an incorrect password, the server first performs a `bcrypt.compareSync()` operation (~74ms average) before responding. This ~4.4× timing difference is trivially detectable even over a network — a single request suffices.

The endpoint has no rate limiting or account lockout mechanism, enabling rapid automated enumeration.

Details

In `server/api/controllers/access-tokens/create.js`:

```
// Line 36-40: User not found → IMMEDIATE error (no bcrypt)
const user = await sails.helpers.users.getOneByEmailOrUsername(inputs.emailOrUsern
if (!user) {
  throw Errors.INVALID_USERNAME_PASSWORD; // ~17ms avg
}

// Line 43-45: User found → bcrypt comparison THEN error
if (!bcrypt.compareSync(inputs.password, user.password)) {
```

```
  throw Errors.INVALID_USERNAME_PASSWORD; // ~74ms avg
}
```

While both paths return the same HTTP 401 error message (`"Invalid username or password"`), the timing difference created by the presence or absence of `bcrypt.compareSync()` is a reliable oracle.

Impact

- **User enumeration**: Attacker can determine which email addresses have accounts on the instance
- **Credential stuffing preparation**: Enumerated valid accounts can be targeted for password attacks
- **No rate limiting**: The endpoint allows unlimited attempts, enabling rapid enumeration of large email lists
- **No account lockout**: Failed login attempts do not trigger any lockout or notification

Remediation

1. **Add constant-time comparison**: Perform a dummy bcrypt operation when the user is not found:

```
const DUMMY_HASH = bcrypt.hashSync('dummy', 10);

if (!user) {
  bcrypt.compareSync(inputs.password, DUMMY_HASH); // constant time
  throw Errors.INVALID_USERNAME_PASSWORD;
}
```

2. **Add rate limiting** on the authentication endpoint (e.g., 5 attempts per minute per IP)
3. **Add account lockout** after N consecutive failed attempts

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

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

Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-41418

Weaknesses

▶ CWE-208

Credits

QiaoNPC	Reporter
Across-Verticals-Malaysia	Other