Vulnerability Report

Title: IDOR allows authenticated users to view other users' action history entries

Summary

An authenticated user can view **action history (audit log) entries belonging to other users** by modifying the numeric identifier in the following endpoint:

```
https://admin.alwaysdata.com/log/{log_id}/detail/
```

The application does not verify ownership of the requested action history entry, resulting in **horizontal privilege escalation** and **unauthorized read-only disclosure of user data**.

Scope

- https://admin.alwaysdata.com

Affected Endpoint

```
GET https://admin.alwaysdata.com/log/{log_id}/detail/
```

Proof of Concept (Steps to Reproduce)

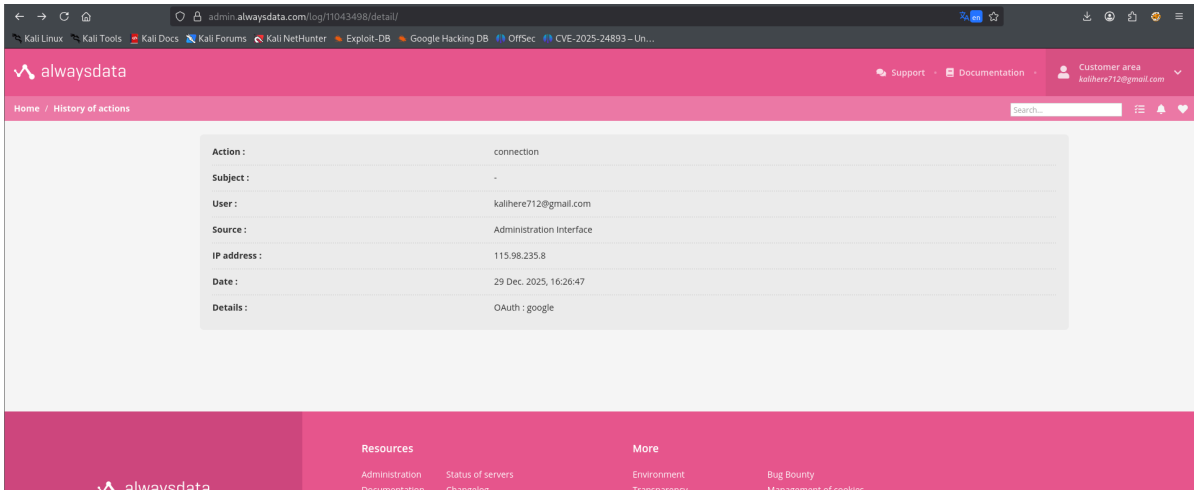
1. Log in to `https://admin.alwaysdata.com` using a valid account.
2. Navigate to the **History of actions** page:

   ```
   https://admin.alwaysdata.com/log/
   ```

3. Click the 🔍 (details) icon for one of your own action history entries.
4. You are redirected to a URL similar to:

```
https://admin.alwaysdata.com/log/11043498/detail/
```

5. Confirm that the displayed action history entry belongs to your account.
   [Screenshot 1: My own action history entry]

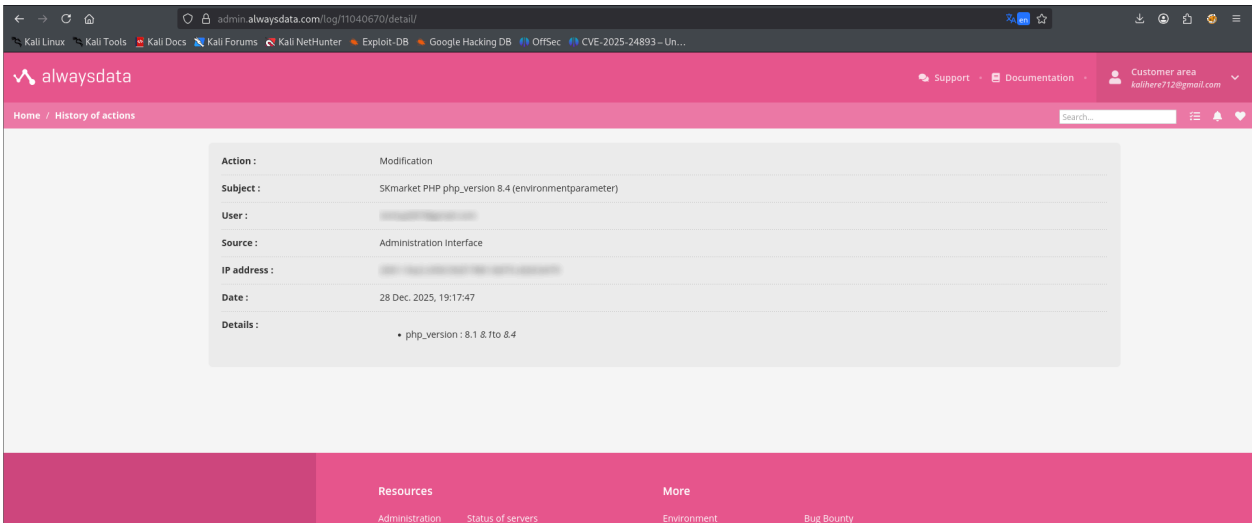


6. Modify the numeric `log_id` value in the URL to another valid identifier:

```
https://admin.alwaysdata.com/log/11040670/detail/
```

7. Observe that the application displays an **action history entry belonging to another user**, without any authorization error.

   [Screenshot 2: Action history detail belonging to another user (email and IP address redacted)]



Observed Result

- The server responds with **HTTP 200 OK**
- An action history entry belonging to a **different user** is displayed

The disclosed information includes:

- User email address
- IP address (IPv4 / IPv6)
- Authentication method (e.g. OAuth Google)
- Timestamp of the action
- Source of the action (Administration Interface)

Expected Result

Users should only be able to view **their own** action history entries.

Requests for action history entries not owned by the authenticated user should return:

- `403 Forbidden`

  or

- `404 Not Found`

Impact

- **Unauthorized read-only access to other users’ action history entries**
- Disclosure of sensitive personal information (email addresses, IP addresses)
- Disclosure of authentication methods and account activity
- **Horizontal privilege escalation**
- Violation of user privacy and confidentiality

Due to the predictable nature of the numeric identifier, this issue is **enumerable in theory**, although testing was intentionally limited to a minimal proof of concept in accordance with the program rules.