🧪 Proof of Concept (PoC)

✅ Prerequisites

- Valid login credentials for a low-privileged user
- Access to the `/locations/{id}/printassigned` endpoint

🔁 Steps to Reproduce

1. Log in as a user assigned to a specific department/location.
2. Navigate to the following URL:

https:///locations/2/printassigned

Where `2` is the location assigned to the current user.

3. Modify the URL manually and change the location ID to another department:

https:///locations/1/printassigned

4. You will now be able to see assets assigned to **other departments**, violating access control policies.

🔐 Impact

- **Confidentiality Violation**: Unauthorized access to sensitive asset data across departments
- **Information Disclosure**: Inventory exposure, asset assignments of unrelated business units

🧩 Root Cause

The endpoint `/locations/{id}/printassigned` does not enforce proper **authorization** checks to restrict access by department.

🩹 Patch

The issue was fixed in version **v8.1.0**. Patch reference:
grokability/snipe-it#16672

📚 References

- Fix Commit
- Release Notes

🪪 CVE Information

- **CVE-ID**: CVE-2025-47226
- **Vulnerability Type**: Incorrect Access Control (IDOR)
- **Attack Vector**: Local (authenticated access)
- **Discoverer**: Sn1p3r-H4ck3r