New issue

POST /defUser/pageUser` 中的访问控制漏洞可导致跨组织用户枚举 #403

Open

SeTG-git opened 3 weeks ago

[CVE请求] `POST /defUser/pageUser` 中的访问控制漏洞可导致跨组织用户枚举

摘要

`lamp-cloud` 的端点 `POST /defUser/pageUser`（`DefUserController#pageUser`）存在一个访问控制漏洞。经过身份验证的低权限用户可以枚举其所在组织/公司范围之外的用户。

这似乎是一个行级授权/数据范围失败（BOLA/IDOR 式的读取暴露），而不仅仅是端点认证问题。

产品

- 项目：`dromara/lamp-cloud`
- 组件：`lamp-system-controller` / `lamp-system-biz`
- 端点：`POST /defUser/pageUser`

受影响版本

- 验证版本：`5.8.1`（本地动态验证环境）
- 可能受影响的版本：`DefUserMapper.pageUser` 缺少组织/公司/员工范围谓词的版本。

漏洞类型

- CWE-285：授权不当
- CWE-359：向未经授权的行为者泄露私人个人信息

影响

具有端点权限的普通认证账户可以列出本应不在范围之内的用户（包括高权限/系统账户），从而导致用户资料数据的未授权泄露。

前提条件

- 攻击者拥有任何可以通过 `POST /defUser/pageUser` 端点权限检查的账户。
- 一旦授予端点权限，数据越界访问无需管理员权限。

复现步骤

1. 使用具有 `pageUser` 端点权限的普通账户进行身份验证。
2. 调用：
   - `POST /defUser/pageUser`
   - 正文: `{"current":1,"size":20,"model":{}}`
3. 观察返回的记录，其中包括调用者所在组织/公司之外的用户（例如，`lamp`、`superAdmin`）。

证明（动态验证）

- 呼叫者账户 (`test1`) 公司： `1451532773234835456`
- 包含的回流用户：
  - `lamp`（公司 `1451532727697276928`）
  - `超级管理员` (公司 `1451532667655815168`)
- 这表明存在跨范围的数据暴露问题。

预期行为

`/defUser/pageUser` 应仅返回授权数据范围内的用户（例如，同一组织/公司、角色范围或明确的策略范围）。

实际行为

`/defUser/pageUser` 返回宽泛的用户结果，而不强制实施调用者绑定的员工/组织/公司约束。

技术根本原因

代码路径：

- `DefUserController#pageUser` -> `DefUserServiceImpl#pageUser` -> `DefUserManagerImpl#pageUser` -> `DefUserMapper.xml#pageUser`

在 SQL（`mapper_system/ext/tenant/DefUserMapper.xml`）中，查询仅对 `u.username/nick_name/email/mobile/id_card/state` 应用可选过滤器。
虽然有 `LEFT JOIN base_employee ut on u.id = ut.user_id`，但没有使用调用者上下文（`employeeId`、`companyId`、组织关系等）的行级谓词。

建议的补救措施

1. 在 `pageUser` SQL/服务层中实施行级数据范围控制，例如：
   - 从令牌上下文中绑定调用者的 `员工ID/公司ID/部门ID`，
   - 连接 `base_employee_org_rel` / 组织树 / 角色数据范围策略，
   - 仅将结果限制在授权范围内。
2. 为特权/全局列表行为添加服务器端授权保护。
3. 添加回归测试：
   - 低权限用户无法查看跨公司用户，
   - 管理员行为仍受到明确控制。

安全严重程度

- 建议：**高**（保密性影响、广泛的用户枚举、潜在的权限链）。

CVE请求

请评估此问题，若确认，请请求/分配一个CVE ID。

记者笔记

如果您愿意，我可以私下提供完整的请求/响应证据和经过清理的概念验证（PoC）详细信息。

[CVE Request] Broken Access Control in `POST /defUser/pageUser` Enables Cross-Organization User Enumeration

Summary

A broken access control vulnerability exists in `lamp-cloud` at endpoint `POST /defUser/pageUser` (`DefUserController#pageUser`).
An authenticated low-privilege user can enumerate users outside their own organization/company scope.

This appears to be a row-level authorization/data-scope failure (BOLA/IDOR-style read exposure), not merely an endpoint authentication issue.

Product

- Project: `dromara/lamp-cloud`
- Component: `lamp-system-controller` / `lamp-system-biz`
- Endpoint: `POST /defUser/pageUser`

Affected Version

- Verified on: `5.8.1` (local dynamic validation environment)
- Potentially affected: versions where `DefUserMapper.pageUser` lacks org/company/employee scope predicates.

Vulnerability Type

- CWE-285: Improper Authorization
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor

Impact

A normal authenticated account with endpoint permission can list users that should be out of scope (including high-privilege/system accounts), causing unauthorized disclosure of user profile data.

Preconditions

- Attacker has any account that can pass endpoint permission check for `POST /defUser/pageUser`.
- No admin privileges are required for data overreach once endpoint permission is granted.

Reproduction Steps

1. Authenticate as a normal account with `pageUser` endpoint permission.
2. Call:
   - `POST /defUser/pageUser`
   - Body: `{"current":1,"size":20,"model":{}}`

3. Observe returned records include users outside caller's organization/company (e.g., `lamp`, `superAdmin`).

Proof (Dynamic Validation)

- Caller account (`test1`) company: `1451532773234835456`
- Returned users included:
  - `lamp` (company `1451532727697276928`)
  - `superAdmin` (company `1451532667655815168`)
- This demonstrates cross-scope data exposure.

Expected Behavior

`/defUser/pageUser` should only return users within authorized data scope (e.g., same org/company, role scope, or explicit policy scope).

Actual Behavior

`/defUser/pageUser` returns broad user results without enforcing caller-bound employee/org/company constraints.

Technical Root Cause

Code path:

- `DefUserController#pageUser` -> `DefUserServiceImpl#pageUser` -> `DefUserManagerImpl#pageUser` -> `DefUserMapper.xml#pageUser`

In SQL (`mapper_system/ext/tenant/DefUserMapper.xml`), query only applies optional filters on `u.username/nick_name/email/mobile/id_card/state`.
Although there is `LEFT JOIN base_employee ut on u.id = ut.user_id`, there is no row-level predicate using caller context (`employeeId`, `companyId`, org relations, etc.).

Suggested Remediation

1. Enforce row-level data scope in `pageUser` SQL/service layer, e.g.:
   - bind caller `employeeId/companyId/deptId` from token context,
   - join `base_employee_org_rel` / org tree / role data-scope policies,
   - restrict results to authorized scope only.
2. Add a server-side authorization guard for privileged/global listing behavior.
3. Add regression tests:
   - low-priv user cannot view cross-company users,

- admin behavior remains explicitly controlled.

Security Severity

- Suggested: **High** (confidentiality impact, broad user enumeration, potential privilege-chaining).

CVE Request

Please assess and, if confirmed, request/assign a CVE ID for this issue.

Reporter Notes

I can provide full request/response evidence and sanitized PoC details privately if preferred.

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants