



# WordPress KiviCare plugin <= 3.6.6 - Insecure Direct Object References (IDOR) vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2024-35659  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Patchstack  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2024-06-08 16:15:09 UTC   |
| <b>Updated</b>         | 2026-04-01 16:17:16 UTC   |
| <b>Description</b>     | Missing Authorization vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows Exploiting Incorrect |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-862 | CWE-862 Missing Authorization

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                  | Version | Update | Edition | Language |
|-------------|------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Iqonic</a> | <a href="#">Kivicare</a> | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor                        | Product                  | Version               | Platforms     |
|--------|-------------------------------|--------------------------|-----------------------|---------------|
| CNA    | <a href="#">Iqonic Design</a> | <a href="#">KiviCare</a> | affected 3.6.6 custom | Not specified |

### References

| Reference   | Source                               | Link  |
|---|--------------------------------------|---|
| <a href="https://patchstack.com/database/vulnerability/kivicare-clinic-management-system/wordpress-plugin-kivicare-clinic-management-system/">patchstack.com/database/vulnerability/kivicare-clinic-management-system/word...</a> | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">patchstack.com</a>                  |
| <a href="https://patchstack.com/database/Wordpress/Plugin/kivicare-clinic-management-system/vulnerability/">patchstack.com/database/Wordpress/Plugin/kivicare-clinic-management-system/v...</a>                                   | audit@patchstack.com                 | <a href="#">patchstack.com</a>                  |
| CVE Program record  | CVE.ORG                              | <a href="https://www.cve.org">www.cve.org</a>   |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a> |

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Van Lyubov | Patchstack Bug Bounty Program (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)