



# WordPress Diza theme <= 1.3.9 - Local File Inclusion Vulnerability

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2025-52729                                                                                                             |
| <b>State</b>           | PUBLISHED                                                                                                                  |
| <b>Assigner</b>        | Patchstack                                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2025-06-27 12:15:41 UTC                                                                                                    |
| <b>Updated</b>         | 2026-04-23 15:32:05 UTC                                                                                                    |
| <b>Description</b>     | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in t |

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from audit@patchstack.com

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

**Problem Types:** CWE-98 | CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | audit@patchstack.com | Secondary | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1     | CNA                  | CVSS      | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor  | Product | Version               | Platforms     |
|--------|---------|---------|-----------------------|---------------|
| CNA    | Thembay | Diza    | affected 1.3.9 custom | Not specified |

References

| Reference                                                                       | Source               | Link           | Tags          |
|---------------------------------------------------------------------------------|----------------------|----------------|---------------|
| patchstack.com/database/Wordpress/Theme/diza/vulnerability/wordpress-diza-1-... | audit@patchstack.com | patchstack.com |               |
| CVE Program record                                                              | CVE.ORG              | www.cve.org    | canonical     |
| NVD vulnerability detail                                                        | NVD                  | nvd.nist.gov   | canonical, au |

Vendor Comments And Credit

Discovery Credit

**CNA:** Tran Nguyen Bao Khanh (VCI - VNPT Cyber Immunity) | Patchstack Bug Bounty Program (en)

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