# WordPress Diza theme <= 1.3.15 - Local File Inclusion vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2025-68544 |
| **State** | PUBLISHED |
| **Assigner** | Patchstack |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2025-12-23 12:15:45 UTC |
| **Updated** | 2026-04-23 15:35:59 UTC |
| **Description** | 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 7.5 HIGH from audit@patchstack.com

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

**EPSS:** 0.000800000 probability, percentile 0.236710000 (date 2026-04-23)

**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 | 7.5 | HIGH | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 7.5 | HIGH | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Thembay | Diza | affected 1.3.15 custom | Not specified |

## References

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

## Vendor Comments And Credit

Discovery Credit

**CNA:** João Pedro S Alcântara (Kinorth) | Patchstack Bug Bounty Program (en)

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