



# WordPress Live Dashboard plugin <= 0.3.3 - Reflected Cross Site Scripting (XSS) vulnerability

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

## Summary

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-23474                                                                                                               |
| State           | PUBLISHED                                                                                                                    |
| Assigner        | Patchstack                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                 |
| Published       | 2025-02-14 13:15:43 UTC                                                                                                      |
| Updated         | 2026-04-23 15:23:47 UTC                                                                                                      |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mike Martel Live Dashl |

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from audit@patchstack.com

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

**Problem Types:** CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | audit@patchstack.com | Secondary | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

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

Vendor Declared Affected Products

| Source | Vendor      | Product        | Version               | Platforms     |
|--------|-------------|----------------|-----------------------|---------------|
| CNA    | Mike Martel | Live Dashboard | affected 0.3.3 custom | Not specified |

References

| Reference                                                                       | Source               | Link           | Tags           |
|---------------------------------------------------------------------------------|----------------------|----------------|----------------|
| patchstack.com/database/Wordpress/Plugin/live-dashboard/vulnerability/wordpr... | audit@patchstack.com | patchstack.com |                |
| CVE Program record                                                              | CVE.ORG              | www.cve.org    | canonical      |
| NVD vulnerability detail                                                        | NVD                  | nvd.nist.gov   | canonical, and |

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.