



# WordPress Plant - Gardening & Houseplants WordPress Theme <= 1.0.0 - Sensitive Data Exposure Vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-31051
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-01-07 02:13:42 UTC
<b>Updated</b>	2026-04-28 19:30:56 UTC
<b>Description</b>	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in EngoTheme Plant - Gardening

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from audit@patchstack.com

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

**EPSS:** 0.000280000 probability, percentile 0.078730000 (date 2026-04-28)

**Problem Types:** CWE-497 | CWE-497 CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	EngoTheme	Plant - Gardening Houseplants WordPress Theme	affected n/a 1.0.0 custom	Not specified

### References

#### Reference

[patchstack.com/database/wordpress/theme/plant/vulnerability/wordpress-plant-...](https://patchstack.com/database/wordpress/theme/plant/vulnerability/wordpress-plant-...)

<https://patchstack.com/database/wordpress/theme/plant/vulnerability/wordpress-plant-gardening-houseplants-wordpress-theme-1-0-0-sensitiv>

CVE Program record

NVD vulnerability detail

### 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.

© 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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)