



# WordPress canvasio3D Light plugin <= 2.5.0 - Arbitrary File Upload vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

## Summary

|                 |                                              |
|-----------------|----------------------------------------------|
| CVE             | CVE-2024-34411                               |
| State           | PUBLISHED                                    |
| Assigner        | Patchstack                                   |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published       | 2024-05-14 15:38:52 UTC                      |
| Updated         | 2026-04-28 19:25:21 UTC                      |

**Description**      Unrestricted Upload of File with Dangerous Type vulnerability in Thomas Scholl canvasio3D Light.This issue affects canvas

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from audit@patchstack.com

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

**EPSS:** 0.007600000 probability, percentile 0.734210000 (date 2026-04-28)

**Problem Types:** CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | audit@patchstack.com | Secondary | 9.9   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |
| 3.1     | CNA                  | CVSS      | 9.9   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor        | Product          | Version                   | Platforms     |
|--------|---------------|------------------|---------------------------|---------------|
| CNA    | Thomas Scholl | Canvasio3D Light | affected n/a 2.5.0 custom | Not specified |

References

| Reference                                                                       | Source                               | Link         |
|---------------------------------------------------------------------------------|--------------------------------------|--------------|
| patchstack.com/database/vulnerability/canvasio3d-light/wordpress-canvasio3d-... | af854a3a-2127-422b-91ae-364da2661108 | patchstack.c |
| CVE Program record                                                              | CVE.ORG                              | www.cve.org  |
| NVD vulnerability detail                                                        | NVD                                  | nvd.nist.gov |

Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter (Patchstack Alliance) (en)

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