



# Materialis Companion <= 1.3.41 - Authenticated (Contributor+) Store Cross-Site Scripting via materialis\_contact\_form Shortcode

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2024-4707   |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Wordfence   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2024-06-06 04:15:13 UTC   |
| <b>Updated</b>         | 2026-04-08 18:21:54 UTC   |
| <b>Description</b>     | The Materialis Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's materialis_cont |

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

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

| Version | Source                 | Type      | Score | Severity | Vector                                       |
|---------|------------------------|-----------|-------|----------|--|
| 3.1     | nvd@nist.gov           | Primary   | 5.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N |
| 3.1     | security@wordfence.com | Secondary | 6.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |
| 3.1     | CNA                    | DECLARED  | 6.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                       | Product                              | Version | Update | Edition | Language |
|-------------|------------------------------|--------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Extendthemes</a> | <a href="#">Materialis Companion</a> | All     | All    | All     | All      |

#### Vendor Declared Affected Products

| Source | Vendor                       | Product                              | Version                | Platforms     |
|--------|------------------------------|--------------------------------------|------------------------|---------------|
| CNA    | <a href="#">Horearadu</a>    | <a href="#">Materialis Companion</a> | affected 1.3.41 semver | Not specified |
| ADP    | <a href="#">Extendthemes</a> | <a href="#">Materialis Companion</a> | affected 1.3.41 semver | Not specified |

#### References

| Reference   | Source                               | Link               |
|---|--------------------------------------|--------------------|
| <a href="https://plugins.trac.wordpress.org/browser/materialis-companion/trunk/theme-data/materialis/func...">plugins.trac.wordpress.org/browser/materialis-companion/trunk/theme-data/materialis/func...</a> | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">pl</a> |
| <a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/6ca4dff0-ca3a-44cf-a30b-36b31...">www.wordfence.com/threat-intel/vulnerabilities/id/6ca4dff0-ca3a-44cf-a30b-36b31...</a>                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">w</a>  |
| <a href="https://plugins.trac.wordpress.org/changeset">plugins.trac.wordpress.org/changeset</a>   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">pl</a> |
| CVE Program record  | CVE.ORG                              | <a href="#">w</a>  |
| NVD vulnerability detail  | NVD                                  | <a href="#">n</a>  |

#### Vendor Comments And Credit

Discovery Credit

**CNA:** [Matthew Rollings \(en\)](#)

#### Additional Advisory Data

| Source | Time                     | Event     |
|--------|--------------------------|-----------|
| CNA    | 2024-06-05T15:30:15.000Z | Disclosed |

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

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)