



# WordPress OneStore Sites plugin <= 0.1.1 - CSRF to Arbitrary Plugin Installation vulnerability

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2025-25107                                                                                                          |
| <b>State</b>           | PUBLISHED                                                                                                               |
| <b>Assigner</b>        | Patchstack                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2025-02-07 10:15:16 UTC                                                                                                 |
| <b>Updated</b>         | 2026-04-01 17:18:23 UTC                                                                                                 |
| <b>Description</b>     | Cross-Site Request Forgery (CSRF) vulnerability in sainwp OneStore Sites onestore-sites allows Cross Site Request Forge |

## Risk And Classification

**Problem Types:** CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

## Vendor Declared Affected Products

| Source | Vendor                 | Product                        | Version               | Platforms     |
|--------|------------------------|--------------------------------|-----------------------|---------------|
| CNA    | <a href="#">Sainwp</a> | <a href="#">OneStore Sites</a> | affected 0.1.1 custom | Not specified |

## References

| Reference                                                                                       | Source                                                         | Link                           | Tags           |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------|----------------|
| <a href="#">patchstack.com/database/Wordpress/Plugin/onestore-sites/vulnerability/wordpr...</a> | <a href="mailto:audit@patchstack.com">audit@patchstack.com</a> | <a href="#">patchstack.com</a> |                |
| CVE Program record                                                                              | CVE.ORG                                                        | <a href="#">www.cve.org</a>    | canonical      |
| NVD vulnerability detail                                                                        | NVD                                                            | <a href="#">nvd.nist.gov</a>   | canonical, ana |

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Abdi Pranata | Patchstack Bug Bounty Program (en)

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](https://cve.report/api)

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