



INTEGRITY LABS



- [Home](#)
- [Articles](#)
- [Advisories](#)
- [Tools](#)
- [VDP](#)
- [About](#)

September 07, 2022

# CVE-2022-37250 - Stored XSS in User Addresses Title in Craft CMS

## 1. Vulnerability Properties

**Title:** Stored XSS in User Addresses Title in Craft CMS

**CVE ID:** CVE-2022-37250

**CVSSv3 Base Score:** 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

**Vendor:** Craft CMS

**Products:** Craft CMS

**Advisory Release Date:** 7 Sep 2022

**Advisory URL:** <https://labs.integrity.pt/advisories/cve-2022-37250>

**Credits:** Discovery by Gil Correia <gil.correia[at]devoteam.com>

## 2. Vulnerability Summary

For this XSS the attacker needs to create a new user and associate the Field “Addresses” to the new user. From there, the attacker should go to the path /admin/myaccount, select the new user and Add an address. Now the title should contain the new xss payload, and hit the save button. The javascript code runs now everytime a victim does a GET request to /admin/myaccount.

## 3. Vulnerable Versions

- 4.2.0.1

## 4. Solution

- Update to version 4.2.1 or higher

## 5. Vulnerability Timeline

- 29/07/22 -Vulnerability reported to Craft CMS via their report page.
- 29/07/22 -Vulnerability verified by vendor.
- 29/07/22 -Vulnerability fixed by vendor
- 07/09/22 -Advisory released.

## 6. References

- <https://github.com/craftcms/cms/commit/cdc9cb66d0716c9552e4113c8e426fd1a31f9516>

[CVE-2022-37248 - Stored XSS in Field Layout in Craft CMS](#)

[CVE-2022-37251 - Stored XSS in Drafts in Craft CMS](#)

---

### Latest Advisories

- [CVE-2022-37721 - Stored Cross-Site Scripting in PyroCMS](#)
- [CVE-2022-37720 - Stored Cross-Site Scripting in OrchardCMS](#)
- [CVE-2022-37251 - Stored XSS in Drafts in Craft CMS](#)
- [CVE-2022-37250 - Stored XSS in User Addresses Title in Craft CMS](#)
- [CVE-2022-37248 - Stored XSS in Field Layout in Craft CMS](#)

### Latest Articles

- [The Curious Case of Apple iOS IKEv2 VPN On Demand](#)
  - [Gmail Android app insecure Network Security Configuration.](#)
  - [Reviewing Android Webviews fileAccess attack vectors.](#)
  - [Droidstat-X, Android Applications Security Analyser Xmind Generator](#)
  - [Uber Hacking: How we found out who you are, where you are and where you went!](#)
- 

© 2022 Integrity Part of Devoteam. All rights reserved. | [Cookie Policy](#)

### Cookie Consent X

Integrity S.A. uses cookies for analytical and more personalized information presentation purposes, based on your browsing habits and profile. For more detailed information, see our [Cookie Policy](#).

Accept