September 07, 2022

CVE-2022-37248 - Stored XSS in Field Layout in Craft CMS

1. Vulnerability Properties

Title: Stored XSS in Field Layout in Craft CMS
CVE ID: CVE-2022-37248
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-2022-37248
Credits: Discovery by Gil Correia <gil.correia[at]devoteam.com>

2. Vulnerability Summary

The procedure to replicate this XSS occurs everytime the “Field Layout” is loaded. The attacker adds a “New Tab” with the payload, saves the field Layout and the stored XSS is now created. This affects the following pages:
• /admin/settings/sections//entrytypes/ • /admin/settings/globals/ • /admin/settings/categories/ • /admin/settings/tags/ • /admin/settings/assets/volumes/ • /admin/settings/users • /admin/settings/fields

3. Vulnerable Versions

- 4.2.0.1

4. Solution

- Update to version 4.2.1 or higher

5. Vulnerability Timeline

- 28/07/22 -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/cedeba0609e4b173cd584dae7f33c5f713f19627

CVE-2022-37247 - Stored XSS in Fields in Craft CMS
CVE-2022-37250 - Stored XSS in User Addresses Title 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!
