November 14, 2022

CVE-2022-37720 - Stored Cross-Site Scripting in OrchardCMS

1. Vulnerability Properties

Title: Stored Cross-Site Scripting in OrchardCMS
CVE ID: CVE-2022-37720
CVSSv3 Base Score: 8.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)
Vendor: Orchard Project
Products: OrchardCMS
Advisory Release Date: 14 November 2022
Advisory URL: https://labs.integrity.pt/advisories/cve-2022-37720
Credits: Discovery by Bruno Barreirinhas <bb[at]integrity.pt>

2. Vulnerability Summary

OrchardCMS is vulnerable to a stored XSS when a low privileged user such as an author or publisher, injects a crafted html and javascript payload in a blog post, leading to full admin account takeover or privilege escalation when the malicious blog post is loaded in the victim's browser.

3. Vulnerable Versions

- < 1.10.3

4. Solution

No official patch released by the vendor due to discontinued product
*Upgrade to Orchard Core

5. Vulnerability Timeline

- 02/Aug/22 - Vendor contacted via Github
- 02/Aug/22 - Bug reported to vendor
- 03/Aug/22 - Bug verified by vendor
- 03/Aug/22 - Notified the vendor regarding the impact
- 09/Aug/22 - Advised vendor about a potential fix
- 09/Aug/22 - Vendor informs that product is no longer supported
- 07/Sep/22 - Notified vendor about disclosure (no feedback)
- 09/Nov/22 - Notified vendor about disclosure (vendor acknowledged)
- 14/Nov/22 - Advisory Released

6. References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37720

CVE-2022-40904 (To Be Disclosed)
CVE-2022-37721 - Stored Cross-Site Scripting in PyroCMS

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!
