research@STM:~$ cat /stm/vulndb/CVE-2022-30874

CVE-2022-30874

Name
Stored XSS in menu item link

Product name
NukeViet CMS

CVSS score
4.8 (Medium)

Confirmed exploitable versions
< 4.5.02

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

Researcher
Dawid Bakaj

Description
NukeViet CMS allows top menu modification via admin panel. Value passed as new menu item's URL is not properly sanitized, leading to Stored Cross-Site Scripting vulnerability in version 4.5.02 or earlier. Prior administrative access to the website is required for exploitation. Successful attack may result in tampering with data presented to users or exfiltration of information from the victim's current session.

Proof-of-concept

1. Navigate to "Top Menu" section in the admin panel (location: `/admin/index.php?language=en&nv=menu&op=rows&mid=1`).
2. Add item with following values and click Save:
    - Item Name: `XSSTEST`
    - Link: `"> <scr<script>ipt>alert(document.domain)</scr<script>ipt>`
3. Visit the website as a regular non-privileged user or an admin user. XSS alert box should appear.

Voting functionality was also affected by the same vulnerability.

Timeline

- 16-12-2021 - Vulnerability reported to vendor
- 17-12-2021 - First response from vendor
- 04-01-2022 - First fix
- 04-01-2022 - First bypass reported
- 15-03-2022 - Second fix
- 16-03-2022 - Second bypass reported
- 18-03-2022 - Last fix
- 25-06-2022 - Report disclosure

References

https://whitehub.net/submissions/2968

https://github.com/nukeviet/nukeviet/blob/nukeviet4.5/CHANGELOG.txt

research@stmcyber.pl