masquerad3r / **sxss-limesurvey-6.15.20-251021-poc.md**

Created 4 months ago

Code Revisions 1

Stored XSS: Limesurvey <=6.15.20-251021

sxss-limesurvey-6.15.20-251021-poc.md

Authenticated Stored Cross-Site Scripting (SXSS)

Summary

Vulnerable Version	Limesurvey v6.15.20+251021
Category	Injection
CWE	Improper Neutralization of Input During Web Page Generation (CWE-79)
CVSS	8.4 (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H)
Vulnerable Endpoint	`https://DOMAIN/index.php/homepageSettings`
Vulnerable Parameter	`Box[title]` and `Box[url]`

Proof of Concept

NOTE:

- Replace the DOMAIN with appropriate hostname/IP.

- This vulnerability is exploitable for authenticated users, so authenticate before trying to reproduce.

Steps:

1. Visit the `/index.php/homepageSettings` endpoint.
2. Create a new box or update an existing one.
3. Both `Destination URL` and `Title` fields are vulnerable, you can use below payloads for respective fields:
   - `Destination URL`: `" onmouseenter="alert('dest url')" class="btn btn-g-800 btn-icon"><input type="hidden"`
   - `Title`: `New" onmouseenter="alert('title')" fix="`

   NOTE: Pay attention to the used icon which will make it easier to detect the bug later on reflecting page
4. Now visit `/index.php/dashboard/view` and hover over the new created or edited button from Step 2.
5. We see two alert boxes with `dest url` and `title` strings.

Remediation

Upgrade to Limesurvey >=6.15.21+251028