PTT-2026-003 – OctoberCMS – Stored Cross Site Scripting via SVG Filter Bypass

CVE-ID: CVE-2026-25133

Credits:

Matei “Mal” Bădănoiu and Mihai “hust” Radu of Pentest-Tools.com

Environment:

- October CMS v4.1.9

CVSSv3: 4.6 Medium - AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

Note: If an attacker hijacks a superuser, they can achieve RCE, increasing the CVSS score to:

8.0 High - AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Description:

OctoberCMS implements filters to prevent the insertion of Cross-Site Scripting (XSS) payloads in SVG images, but attackers can bypass these filters and upload images that trigger malicious JavaScript payloads when someone accesses them.

Requirements:

In default OctoberCMS setups, the attacker will require a set of valid user credentials to upload images.

Fix:

The vendor patched the vulnerability. The advisory can be found here: https://github.com/advisories/GHSA-gcqv-f29m-67gr

Proof of Concept:

Although the OctoberCMS application has a filter to prevent malicious attributes in SVG that contain JavaScript code, attackers can bypass this filter, resulting in a Stored XSS attack.

SVG filter in “vendor/october/rain/src/Html/HtmlBuilder.php”:

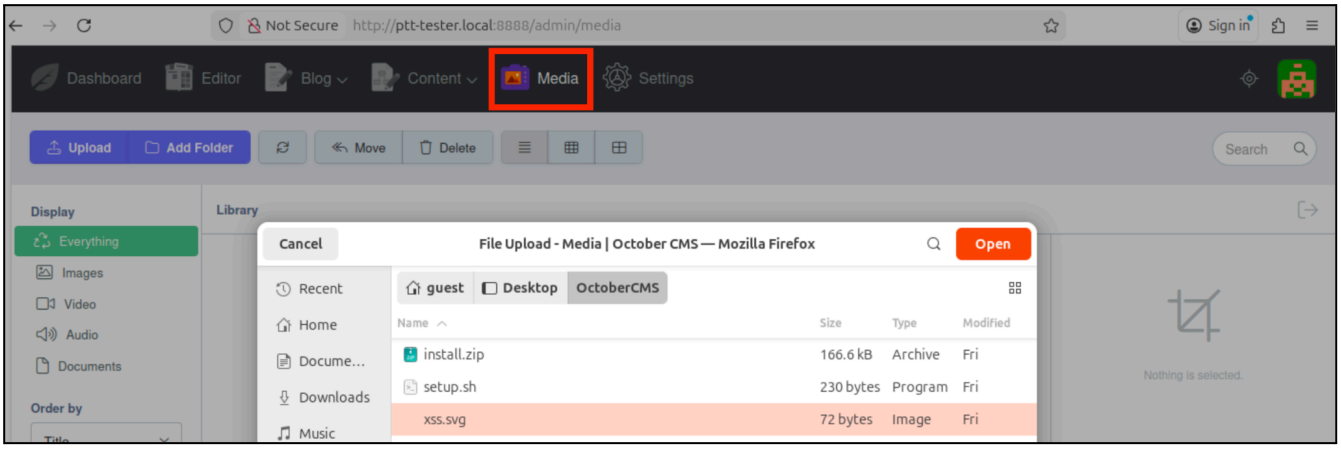
```
// Remove any attribute starting with "on" or xmlns
$html = preg_replace('#(<[^>]+[\x00-\x20\"\'\/])(on)[^>]*>#iUu', "$1>", $html);
```

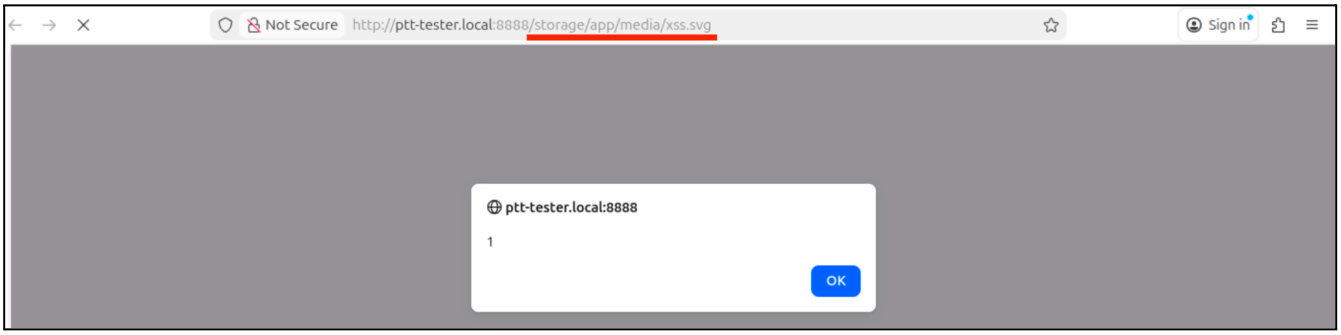
SVG payload that bypasses the filter:

```
<svg xmlns="http://www.w3.org/2000/svg" a=">" onload="alert(1)">
</svg>
```

We identified at least two components that attackers can use to upload or save these malicious SVGs:

- The “Media” Component





- The “Avatar” image of a user:

Note: Although the application won't accept the SVG as a valid image and won't save the changes, the system still uploads the file, and attackers can force legitimate OctoberCMS users to access it via a direct link.

