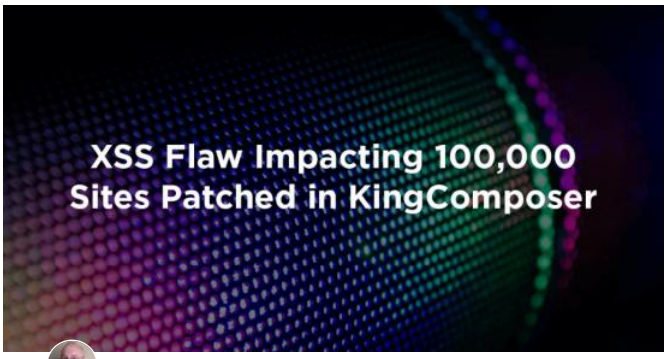

Ram Gall

July 9, 2020

XSS Flaw Impacting 100,000 Sites Patched in KingComposer

On June 15, 2020, our Threat Intelligence team was made aware of a number of access control vulnerabilities that had recently been disclosed in KingComposer, a WordPress plugin installed on over 100,000 sites. During our investigation of these vulnerabilities, we discovered an unpatched reflected Cross-Site Scripting(XSS) vulnerability.

Wordfence Premium customers received a new firewall rule the same day, protecting against the newly patched access control vulnerabilities as well as the unpatched Cross-Site Scripting vulnerability. Wordfence users still using the free version will receive this rule after 30 days, on July 15, 2020.

We attempted to contact the plugin's developers the next day, on June 16, 2020. Since we did not receive a response after 9 days, we contacted the WordPress Plugins team on June 25, 2020. The WordPress Plugins team replied the next day and let us know that they were in touch with the developers of the KingComposer plugin, and a patch was released on June 29, 2020.

What is Reflected Cross-Site Scripting(XSS)?

We've written a number of articles about Stored Cross-Site Scripting(XSS) vulnerabilities in the past, and how they can be used to take over a website if an administrator accesses a page on their site containing a malicious JavaScript. We've also written about Cross-Site Request Forgery(CSRF) attacks, where an attacker can trick a victim into clicking a specially crafted link in order to make changes to a site.

Reflected XSS vulnerabilities have characteristics of both of these vulnerabilities. Much like a CSRF attack, exploiting a Reflected XSS vulnerability usually relies on an attacker tricking their victim into clicking a malicious link which sends the victim to the vulnerable site along with a malicious payload. This can be done in a number of ways, but it is common to first link to an intermediate site controlled by the attacker, which then sends a request containing a malicious payload to the vulnerable site on behalf of the victim.

A notable distinction between the stored XSS vulnerabilities more commonly found and reflected XSS vulnerabilities such as this, is that the malicious scripts that are used as part of the exploit are not actually stored anywhere in the database with reflected XSS vulnerabilities. Rather, the malicious scripts are reflected and executed once during the exploit.

As with Stored XSS attacks, the malicious payload will be executed in the victim's browser. However, with reflected XSS, the vulnerable site would immediately output (reflect) the malicious JavaScript payload, which would be executed a single time in the victim's browser instead of being stored in the database for later execution.

This could be used in a variety of attacks. For instance, if the victim was a logged-in administrator on the vulnerable site, the reflected JavaScript could be used to create a new, malicious administrator account controlled by the attacker.

In order for reflected XSS attacks to successfully exploit a user, an attacker needs to trick the user into performing an action. For that reason, we highly recommend remaining vigilant when clicking on links or attachments in comments, emails, and other communication sources unless you are sure of their integrity and legitimacy.

Description: Reflected Cross-Site Scripting(XSS)
Affected Plugin: Page Builder: KingComposer – Free Drag and Drop page builder by King-Theme
Plugin Slug: kingcomposer
Affected Versions: < 2.9.5
CVE ID: CVE-2020-15299
CVSS Score: 6.1(medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Fully Patched Version: 2.9.5

KingComposer is a WordPress plugin that allows Drag and Drop page building, and it registers a number of AJAX actions to accomplish this. One of these AJAX actions was no longer actively used by the plugin, but could still be used by sending a `POST` request to `wp-admin/admin-ajax.php` with the `action` parameter set to `kc_install_online_preset`.

The vulnerable function:

```
1540 | public function install_online_preset(){
1541 |
1542 |     $data = isset($_POST['kc-online-preset-data']) ? esc_attr($_POST['kc-online-preset-data']) : '';
1543 |     $link = isset($_POST['kc-online-preset-link']) ? esc_url($_POST['kc-online-preset-link']) : '';
1544 |     $link = str_replace( 'http://features.kingcomposer.com/', 'https://kingcomposer.com/presets/', $link);
1545 |     $callback = '
1546 |     <script type="text/javascript">
1547 |         top.kc.cfg.preset_link = "'.$link.'";
1548 |         top.kc.backbone.push(\''.str_replace( "\n", '\'+"\n"+\'', base64_decode($data)).'\');
1549 |         top.kc.tools.popup.close_all();
1550 |     </script>';
1551 |
1552 |     echo $callback;
1553 |
1554 |     exit;
1555 |
1556 | }
```

This function renders a JavaScript based on the contents of the `kc-online-preset-link` and `kc-online-preset-data` parameters. Since it uses the `esc_attr` and `esc_url` functions, it appears safe at first glance. Unfortunately, however, the contents of the `kc-online-preset-data` parameter are base64-decoded *after* this step.

As such, if an attacker used base64-encoding on a malicious payload, and tricked a victim into sending a request containing this payload in the `kc-online-preset-data` parameter, the malicious payload would be decoded and executed in the victim's browser. The patched version of this plugin resolved the issue by removing the vulnerable function entirely.

Disclosure Timeline

patched vulnerabilities in the KingComposer plugin. We release a firewall rule covering both the patched and unpatched vulnerabilities to our Premium users.
June 16, 2020 – We attempt to contact the developers of the KingComposer plugin.
June 25, 2020 – We contact the WordPress Plugins team about the vulnerability.
June 26, 2020 – The WordPress Plugins team responds and indicates that they are in touch with the developers of the KingComposer plugin.
June 29, 2020 – Patched version of KingComposer is released.
July 15, 2020 – Firewall rule becomes available to Wordfence Free users.

Conclusion

In today's blog post, we discussed a Reflected Cross-Site Scripting(XSS) vulnerability in the KingComposer WordPress plugin, and provided some background information on how Reflected XSS attacks work. This vulnerability has been fully patched in version 2.9.5 and we strongly recommend updating to this version immediately. Sites running Wordfence Premium have been protected against this vulnerability, as well as older vulnerabilities in the KingComposer plugin, since June 15, 2020. Sites still using the free version of Wordfence will receive the firewall rule update on July 15, 2020.
Did you enjoy this post? Share it!

Comments

2 Comments

osk3r *
July 13, 2020
4:48 am

Hey, nice work and thanks for letting uns all know / keeping us a bit safer.
I would just love for you to always add a simple example of how a specific vulnerability might potentially be exploited. Maybe without "this code leading to that code ... " stuff I don't understand.
Again, thanks alot and keep up the good work!

Ram Gall *
July 13, 2020
8:19 am

Hi osk3r,
Thank you for your kind words! We've actually got a YouTube video where Chloe hacks a site using XSS (I believe it's a CSRF to stored XSS but it's pretty similar) that shows how this kind of vulnerability can be used to take over a site.
Check out https://www.youtube.com/watch?v=RMDSBlc_yFA starting at about 27:00