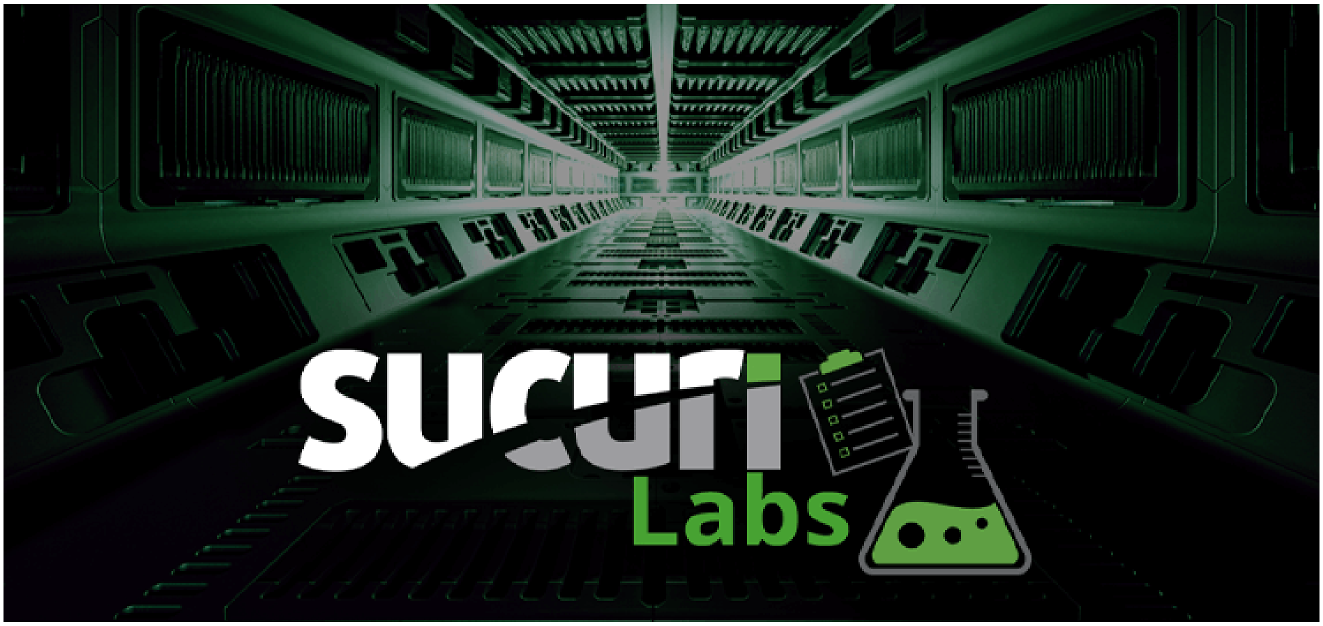
Sucuri Blog

blog.sucuri.net/2020/12/the-dangers-of-using-abandoned-plugins-themes.html

Krasimir Konov

December 17, 2020



It’s not very often that we see abandoned components being used on a website — but when we do, it’s most often because the website was exhibiting malware-like behavior and we were called to investigate and clean up the site.

Old and abandoned plugins and themes are a good target for opportunistic attackers who are looking for any expired domains that might be used by those components. Once an attacker gets a hold of those domains, they’re able to distribute malware to any users that still have that resource installed on their site. Here’s an example of that exact scenario.

Expired Domain for My Weather Plugin

The plugin was called “My Weather” and one of its main functions was to show weather widgets on a website. The data for weather information was retrieved by the plugin from an external domain (*weatherforecastmap[.]com*), which happened to expire.

```
$widget_call_string = 'hxxp://weatherforecastmap[.]com/' . $typeflag;
$widget_call_string .= '.php?zona='.$country_name;
$widget_call_string .= '_'.$city;
$widget_call_string = str_replace(" ", "-", $widget_call_string);
$widget_call_string = strtolower($widget_call_string);

if($fahrenheitflag != 0)
            $widget_call_string = str_replace(".php", "F.php", $widget_call_string);
```

Weather Data Replaced with Malicious Injections

The URL generated by the plugin for the weather data was based on the city and country — for example: **hxxps://weatherforecastmap[.]com/weather3F.php?zona=mexico_playa-del-carmen**

```
echo '<script type="text/javascript" src="'.$widget_call_string . '"></script>';
```

Attackers were able to register the domain and, instead of serving the weather information, they replaced the data source with a malicious JavaScript injection which was loaded on a user's browser whenever they visited a site using the abandoned My Weather plugin.

Unwanted Browser Add-ons & Advertisements

```
var
_0x2cf9=['setA','onerror','rtl','getComputedStyle','direction','classNam
e','left','-99999px','checkScript','complete','readyState','checkBlock',
'detect','trim','clicks','pages','simple','20','0','3','2','0','1','0','
hxxp://fnacgbik9v14[.]com/hdzi0thtzm','&scrHeight=','&tz=','&ship=','&re
s=','runTests','getResults','isEmulate','false','true','hxxps://cdn15.ac
loudimages[.]com/36/template/pu1473410272.pdf','true','true','false','fa
lse','100','exclude','random','[object\x20Array]','key','ppu_exp_','ppu_
clicks_','total_count_','isLocalStorageAvailable','No\x20available\x20st
orage','showOnCounter','ppu_show_on','setStorage',';\x20expires=','toUTC
String','\x20expires=','localStorage','expires','parse','now','cookie','
setItem','addBehavior','save','auth','getItem','#default#userData','load
','getAttribute','removeItem','removeAttribute','storageSupport','code',
'QUOTA_EXCEEDED_ERR','getQuery','pvarr','isDescendant'
...
```

This injection resulted in a redirect to another domain: "hxxp://fnacgbik9v14[.]com/hdzi0thtzm".Upon further investigation, we found that the newly registered domain was distributing malware which tricks the user into installing a malicious component/extension on their browser. Post-install, additional ads were then served from another malicious domain — *terraclicks[.]com*.

This example clearly demonstrates how outdated and abandoned components can put your site at risk. We recommend keeping all software updated to prevent these types of issues from impacting your site's reputation — and if you happen to have a plugin, theme, or component on your site that you aren't using, get rid of it.

Another way to mitigate risk is to add a WAF (Web Application Firewall) to your website. WAFs can prevent many attacks, especially if you have old or outdated plugins which may contain known vulnerabilities — the firewall will be able to virtually patch your software until you get the chance to update or transition to a new one.