Vulnerability Report: Remote File Inclusion (RFI) in Eufy Website

1. Executive Summary:

Vulnerability Type**: Remote File Inclusion (RFI)**

Severity: **Medium**

Reported by: Binay Kumar Dubey

Date Reported: 30 Dec, 2023

2. Vulnerability Details:

A Remote File Inclusion (RFI) vulnerability has been identified on the Eufy website (https://us.eufy.com). The vulnerability allows an attacker to include arbitrary external content, potentially leading to unauthorized access, data disclosure, or other malicious activities. This report provides details of the identified RFI vulnerability and its potential impact.

3. Affected URLs and Parameters:

Affected URL: https://us.eufy.com/pages/series

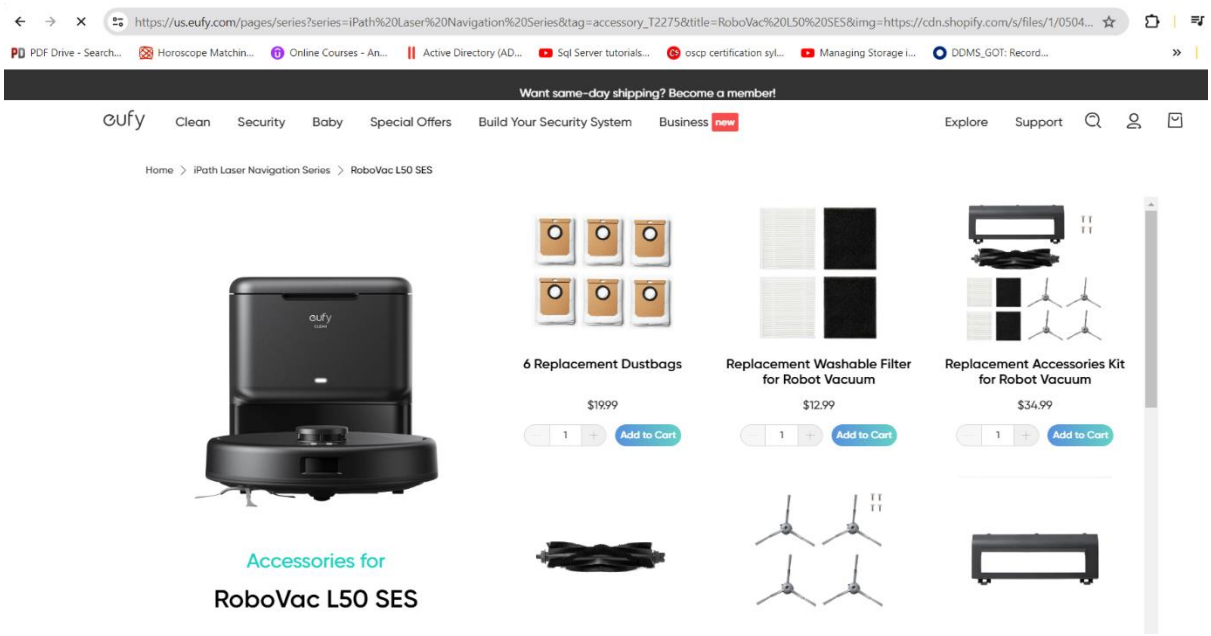
Parameter: img

4. Description:

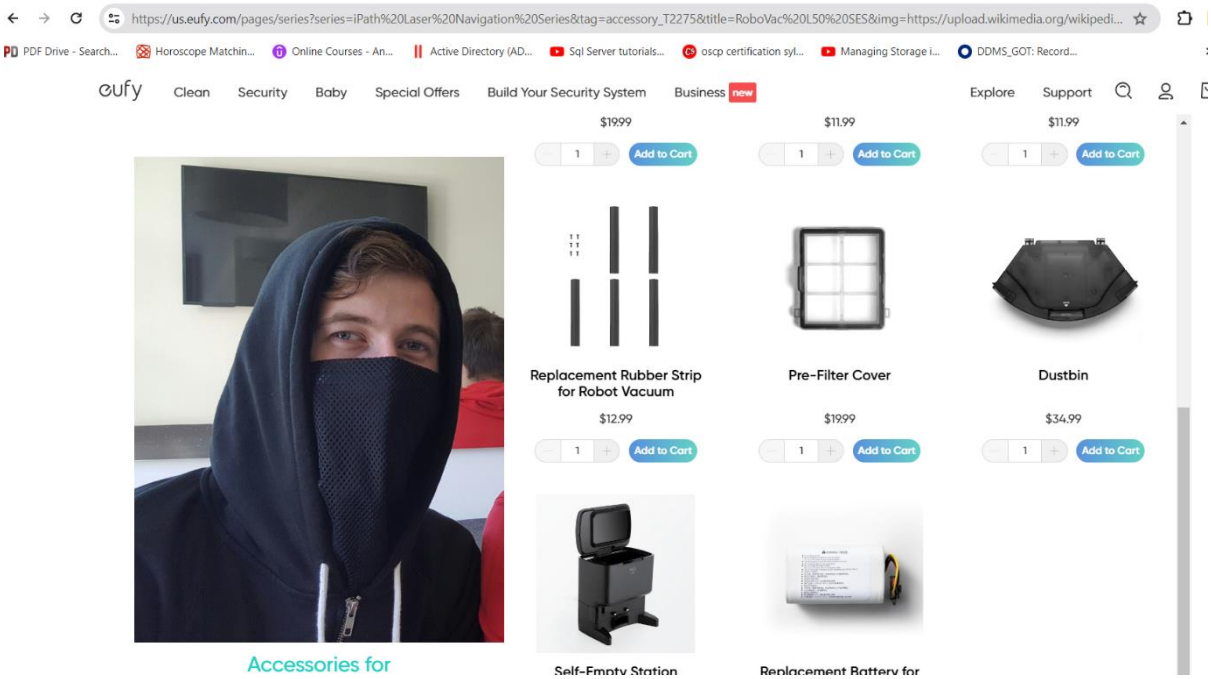
The vulnerability arises from the improper handling of user-controlled input in the "img" parameter within the URL. An attacker can craft a malicious link that includes an external file. This could lead to the display of arbitrary content within the Eufy website, potentially compromising the integrity of the site or exposing users to malicious content.

5. Proof of Concept (PoC):

- The original link: https://us.eufy.com/pages/series?series=iPath%20Laser%20Navigation%20Series&tag=accessory_T2275&title=RoboVac%20L50%20SES&img=https://cdn.shopify.com/s/files/1/0504/7094/4954/files/L50_SES.png?v=1699501176&discontinued=1



- An example of a crafted link exploiting the vulnerability: https://us.eufy.com/pages/series?series=iPath%20Laser%20Navigation%20Series&tag=accessory_T2275&title=RoboVac%20L50%20SES&img=https://upload.wikimedia.org/wikipedia/commons/b/bc/Alan_Walker_%28cropped%29.jpg?v=1699501176&discontinued=1



- In this example, I replaced the original image link with an arbitrary external image link.
- Arbitrary external image link:- https://upload.wikimedia.org/wikipedia/commons/b/bc/Alan_Walker_%28cropped%29.jpg

6. Impact:

- Unauthorized disclosure of external content on the Eufy website.
- Potential for phishing attacks or the display of malicious content to users.

7. Recommendations:

- Implement proper input validation and filtering for user-supplied parameters, especially those used in file inclusions.
- Use a whitelist approach to allow only specific, trusted domains for external content.
- Regularly monitor and log security events related to file inclusions.

8. Acknowledgment:

I would like to acknowledge the prompt response and collaboration of the Eufy website administrators in addressing this security vulnerability.

09. Legal Disclaimer:

This report is submitted in good faith for the purpose of responsible disclosure. The information provided is accurate to the best of my knowledge at the time of reporting.

10. Contact Information:

Binay Kumar Dubey

binaydubey08@gmail.com

Thank you for your attention to this matter. I look forward to your prompt response and the resolution of this vulnerability.

Sincerely,

Binay Kumar Dubey