NF-Security-Team / CVEs Public

Code Issues Pull requests Actions Projects Security Insights

main

CVEs / CVE-OXHOO / Readme.md

Err0r0x41414141 Update Readme.md History

1 contributor

69 lines (44 sloc) | 2.22 KB

Coordinated Disclosure Timeline

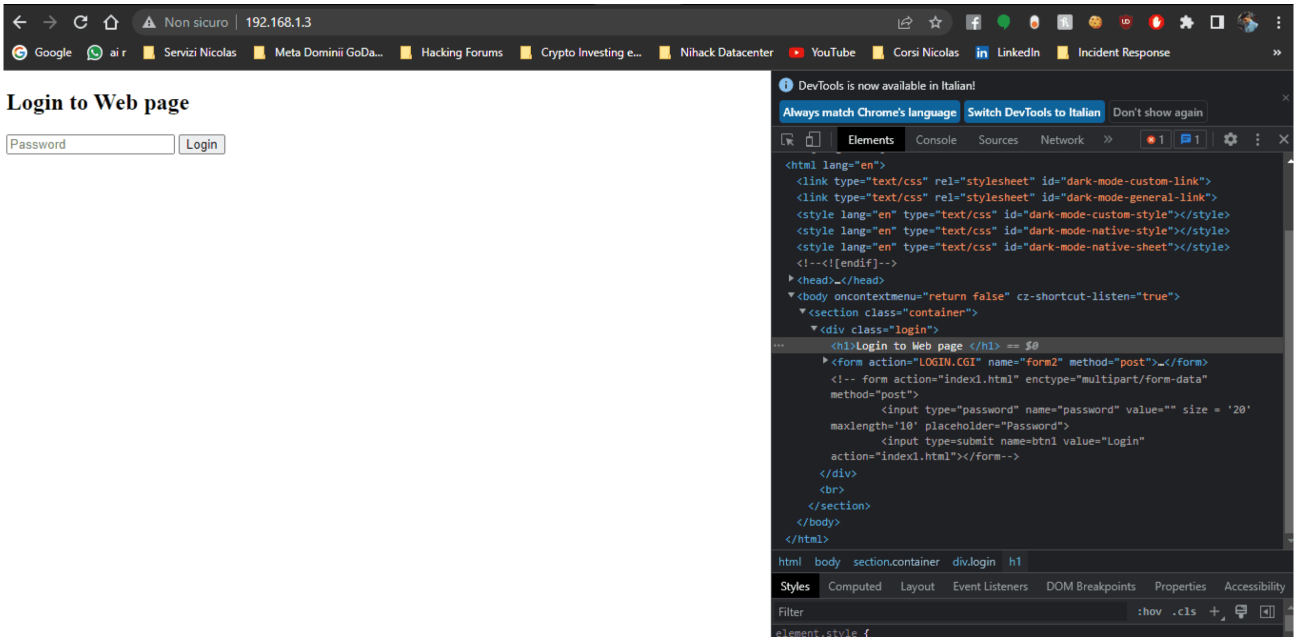
21/09/2022: Report submission to CVE Mitre

Executive Summary

An issue found in "OXHOO TP 50" Web Application, allows attackers to access administrative panel via browsing a specific html page disclosed in login page code.

Technical Summary

To exploit the vulnerability an attacker must read the code of the default login page and notice a commented html reference for "index1.html". By loading that page (http://device_ip/index1.html) the attacker gets administrative access to the device letting him to change an device configuration.



```
<html lang="en">
  <link type="text/css" rel="stylesheet" id="dark-mode-custom-link">
  <link type="text/css" rel="stylesheet" id="dark-mode-general-link">
  <style lang="en" type="text/css" id="dark-mode-custom-style"></style>
  <style lang="en" type="text/css" id="dark-mode-native-style"></style>
  <style lang="en" type="text/css" id="dark-mode-native-sheet"></style>
  <!--<![endif]-->
  <head>…</head>
  <body oncontextmenu="return false" cz-shortcut-listen="true">
    <section class="container">
      <div class="login">
        <h1>Login to Web page </h1> == $0
        <form action="LOGIN.CGI" name="form2" method="post">…</form>
        <!-- form action="index1.html" enctype="multipart/form-data"
        method="post">
                <input type="password" name="password" value="" size = '20'
        maxlength='10' placeholder="Password">
                <input type=submit name=btn1 value="Login"
        action="index1.html"></form-->
      </div>
      <br>
    </section>
  </body>
</html>
element.style {
```

IMPORTANT: this vulnerability allows an attacker to change the device login password.

Product

OXHOO TP 50

Tested Version

OXH1.50

Details

Issue: Unauthenticated access to device's administrative panel

After reaching the default login page provided by device web server look expand all the html page code and look for commented stuff

close to the login form you can see the "index1.html" reference

```
<body oncontextmenu="return false" cz-shortcut-listen="true">

  <section class="container">
    <div class="login">
      <h1>Login to Web page </h1>

          <form action="LOGIN.CGI" name="form2" method="post">
```

```
        <input type="password" name="password" value="" size="20" maxlength="10" placeholder="Password">
                <input type="submit" name="btn1" value="Login" action="LOGIN.CGI">
      </form>
          <!-- form action="index1.html" enctype="multipart/form-data" method="post">
                <input type="password" name="password" value="" size = '20' maxlength='10' placeholder="Password">
                <input type=submit name=btn1 value="Login" action="index1.html"> </form-->
    </div>
        <br>

  </section>



</body>
```

Impact

Unallowed administrative authentication.

CVE

CVE-2022-41436 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41436)

Credit

This issue was discovered and reported by Nicolas Fasolo (@Err0r0x41414141) team Owner of NF_Security (www.threatfeedservice.it).

Contact

You can contact the NF_Security team at info@threatfeedservice.it, please include a reference to CVE-OXHOO in any communication regarding this topic.