Vulnerability Report – Luxul XWR-600 Router
Device Model: Luxul Xen XWR-600 **Interface:** Web Administration UI **Issue Type:** Stored Cross-Site Scripting (XSS)

1. Summary
The XWR-600 devices **Firmware Version** 4.0.1 allows JavaScript to be stored and executed through the SSID name fields. When the SSID value is saved and the page is re-opened, the script runs in the administrator's browser. This is a stored XSS vulnerability.

2. Affected Pages
• Guest Network SSID
• Wireless Profiles (2.4 GHz / 5 GHz)

3. Reproduction Steps

1. Log in to the router web admin page
2. Go to Guest Network or Wireless Profile SSID
3. Enter in SSID field: `"><script>alert(1)</script>`
4. Click Save
5. Re-open the page
   Result: JavaScript alert executes **Expected:** Value should be rendered as text, not executed

4. Impact
An attacker with admin access could:
• Execute JavaScript in the admin browser
• Redirect or inject malicious content

5. Root Cause
User input in SSID fields is stored and rendered without input validation or output encoding. Special characters such as `< > "` are not escaped.

6. Recommended Fix
• Sanitize SSID input values
• Escape HTML characters before rendering
• Apply server-side validation
• Avoid inline script execution

POC's attached: