WESTERMO-18-02: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / **INFORMATIONAL** 2018-05-29

WeOS Vulnerable to Cross Site Request Forgery attack

Description

After investigation, it has been determined that WeOS is open for a Cross-Site Request Forgery (CSRF) attack. The attack uses the fact that the SID is stored in a cookie but requires a user to execute the malicious code.

Affected versions

- 4.13.0 to 4.23.0

Impact

By creating an exploit URL with a specially crafted form, an attacker can force an end user to execute unwanted actions on a web application in which they authenticated. They could for example change the password of the logged in user.

Mitigation

- As a user you can mitigate this CSRF attack by
    - Logging out from the website whenever it's not required
    - Using different browser, one for sensitive, trusted sites and another for general browsing
- Update to the latest firmware when available

Updates

Pending

References

Cross-Site Request Forgery - https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401