Robust Industrial Data Communications –Made Easy

WESTERMO-18-03: Security Advisory

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

Mongoose web server vulnerabilities

CVE

- CVE-2017-11567
- CVE-2017-7185

Description

After investigation it has been determined that WeOS are affected by the following CVE:s:

CVE-2017-11567 is a Cross-site request forgery (CSRF) vulnerability.

CVE-2017-7185 is a Use-after-free vulnerability.

Affected versions

- 4.13.1 to 4.23.0

Impact

CVE-2017-11567 is a Cross-site request forgery (CSRF) vulnerability in Mongoose Web Server that allows remote attackers to hijack the authentication of users for requests. A remote attacker who can lure a Mongoose web server user into clicking a malicious link or visit attacker controlled web page can execute system commands on the system hosting Mongoose server.

CVE-2017-7185 is a Using freed memory attack. The vulnerability is that Mongoose does not properly close connections for malformed requests to the Mongoose server. This can lead to a denial of service (DoS) attack through a crash of the web server.

Severity

CVE-2017-11567: **8.8**
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2017-7185: **7.5**
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Mitigation

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

Updates

Pending

References

CVE-2017-11567 - https://nvd.nist.gov/vuln/detail/CVE-2017-11567
CVE-2017-7185 - https://nvd.nist.gov/vuln/detail/CVE-2017-7185
Cross-Site Request Forgery - https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
Using freed memory - https://www.owasp.org/index.php/Using_freed_memory
Denial of Service - https://www.owasp.org/index.php/Denial_of_Service