Sierra Wireless Security Advisory SWI-PSA-2020-003: Statement on Treck TCP/IP Stack Vulnerabilities

Release Date: June 25, 2020.

Executive Summary:

Sierra Wireless products are not affected by the Ripple20 vulnerabilities which were publicly disclosed on June 16th, 2020.

Issue Description:

Treck TCP/IP stack implementations for embedded systems are affected by multiple vulnerabilities. This set of vulnerabilities was reported by security research firm JSOF. Collectively they are referred to as "Ripple20". Some of these vulnerabilities are also found in the KASAGO TCP/IP middleware suite from Zuken Elmic due to an original partnership between Treck and Elmic Systems.

Details:

Sierra Wireless was contacted by the CERT Coordination Center (CERT/CC) as part of the responsible disclosure process conducted by JSOF after identification of the vulnerabilities. An internal review of products was conducted which concluded that no Sierra Wireless products made use of the affected TCP/IP implementations from Treck and/or Zuken Elmic.

Further Information

For further information about the Ripple20 vulnerabilities:

- JSOF Ripple20 Disclosure: https://www.jsof-tech.com/ripple20/
- Treck Vulnerability Response: https://treck.com/vulnerability-response-information/

For further information and technical support, please contact your authorized reseller or Sierra Wireless representative. To contact Sierra Wireless, please visit https://www.sierrawireless.com/company/contact-us/