Date: July 1, 2020
Subject: Reported vulnerabilities in Treck Inc. Internet Protocol (IP) stack used in multiple Eaton products
Severity rating: Critical (CVSS v3.1)
Product(s): Multiple

Eaton has been notified of multiple vulnerabilities in the Treck Inc. Internet Protocol (IP) stack component used in multiple Eaton products. These vulnerabilities have been collectively published as “Ripple20”. Eaton is evaluating ICS Advisory ICSA-20-168-01 and developing mitigation plans for affected products. Under certain circumstances, the potential exists for these vulnerabilities to allow unauthorized changes to device configurations, denial of service, leakage of previously transmitted data, and in some cases, remote code execution. At this time, the following products manufactured by Eaton’s Power Systems division are known to be affected, when configured with an Ethernet communications interface:

- CL-7 voltage regulator control, all firmware versions
- Form 4D recloser control, all firmware versions
- Form 6 recloser control, firmware versions 4.0 and later
- Edison Idea and IdeaPLUS Relays (all variants), firmware versions 4.0 and later

Eaton is working with Treck and other downstream suppliers to assess the impact of these vulnerabilities on the listed Eaton products. Eaton has published a Security Bulletin based upon an initial impact assessment. Users are encouraged to review this bulletin and sign up for Eaton cybersecurity notifications using the link on our cybersecurity website at http://www.eaton.com/cybersecurity. Additional information on our response to these vulnerabilities will be posted to the cybersecurity notifications section of the Eaton cybersecurity website as it becomes available.

Eaton recommends that customers using the listed products take steps to ensure that system-wide defense-in-depth strategies are exercised as outlined in our whitepaper Cybersecurity considerations for electrical distribution systems. Additional recommendations can be found in ICS Advisory ICSA-20-168-01 and CERT Coordination Center Vulnerability Note VU#257161. Device-specific mitigation actions are anticipated in the form of future firmware updates following additional impact assessment.

Inquiries may be directed to the Eaton Electrical Sector Cybersecurity team at CybersecurityCOE@Eaton.com.
References

i CISA/ICS-CERT Advisory ICSA-20-168-01 (https://www.us-cert.gov/ics/advisories/icsa-20-105-02)


iii Eaton whitepaper WP152002EN (http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&Rendition=Primary&dDocName=WP152002EN)

iv CERT Coordination Center Vulnerability Note VU#257161 (https://kb.cert.org/vuls/id/257161)