Date:	May 14, 2020
Subject:	Reported vulnerability in DNP3 protocol library used in multiple Eaton products
Severity rating:	High (CVSS v3.0)[i]
Product(s):	Multiple

Eaton was notified on April 14, 2020, of a reported buffer overflow vulnerability affecting the Triangle Microworks DNP3 communications protocol stack used in multiple Eaton products. Eaton is evaluating ICS Advisory ICSA-20-105-02[i] and developing mitigation plans for affected products. At this time, the following products manufactured by Eaton's Power Systems division are known to be affected:

- CL-7 voltage regulator control, firmware versions 1.6.0 and later
- Form 4D recloser control, firmware versions 1.7.0 and later
- CBC-8000 capacitor bank control, firmware versions 2.2.3 through 3.2.0
- GridAdvisor Series II smart sensor, firmware versions 1.0.0 and later
- Yukon Feeder Automation software, versions 1.4 through 2.2
- SMP Gateway, software/firmware versions 6.3 through 7.1
- GridServer software, versions 2.0R1 through 2.1R2

Eaton has published a Security Bulletin[ii] 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 this vulnerability will be posted to the cybersecurity notifications section of the Eaton cybersecurity website as it becomes available.

Eaton recommends that customers using these 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[iii]. Additional mitigation actions are anticipated in the form of future firmware and software 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-20-105-02 (https://www.us-cert.gov/ics/advisories/icsa-20-105-02)

[ii] Eaton security bulletin ETN-SB-2020-1001 (https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-security-bulletin-triangle-microwork-dnp3-v1-2.pdf)

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