SAFETY ALERT

Safety Alert No. 394
September 25, 2020

Contact: Stanislaus Kaczmarek
Phone: (703) 787-1612

Recently Discovered Cybersecurity Vulnerabilities May Impact Energy Company Industrial Control Systems

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of multiple vulnerabilities that could allow a highly skilled, remote attacker to take control of various Industrial Control Systems, such as those that open and close valves or control flow rates and pressures.

Therefore, BSEE recommends that operators and contractors follow this CISA guidance:

- Monitor current and future CISA advisories regarding "Treck TCP/IP stack vulnerabilities";
- Assess your potential exposures and take required action to mitigate the risks;
- Notify your Information Technology teams that these vulnerabilities derive from "Treck TCP/IP stack implementations for embedded systems," which CISA believes can impact millions of devices worldwide, including energy sector ICS and a broad scope of internet-connected devices;
- Ensure your vendors notify you of available patches and remediation strategies;
- Review the following products for additional information and mitigations, and update to the latest stable version of Treck TCP/IP stack software (6.0.1.67 or later):
    - CISA's Advisory ICSA-20-168-01
    - CERT Coordination Center's Vulnerability Note VU#257161
    - Treck's Vulnerability Response Information
- Minimize network exposure for all control system devices and/or systems and ensure they are not accessible from the internet;
- Locate control system networks and remote devices behind firewalls and isolate them from the business network;
    - When remote access is required, use secure methods, such as Virtual Private Networks (VPNs).
    - Ensure VPNs are updated to the most current version available as VPN is only as secure as the connected devices.
    - Use an internal DNS server that performs DNS-over-HTTPS for lookups.
- Follow your established internal procedures and report your findings to CISA for tracking and correlation against other incidents if any suspected malicious activity is observed; and,

- Perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA provides a section for control systems security recommended practices on the ICS webpage on us-cert.gov. Several recommended practices are also available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.gov in Technical Information Paper ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Contact Information at CISA

Email: CISAservicedesk@cisa.dhs.gov and Central@cisa.gov

Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://www.us-cert.gov/ics
For incident reporting: https://www.us-cert.gov/report

--BSEE--

A **Safety Alert** is a tool used by BSEE to inform the offshore oil and gas industry of the circumstances surrounding a potential safety issue. It also contains recommendations that could assist avoiding potential incidents on the Outer Continental Shelf.