RISK ALERT

Unauthorized Remote Access to Water Treatment System

February 11, 2021

On February 5 the water supply of the City of Oldsmar in Pinellas County, Florida was attacked by a hacker who increased the concentration of sodium hydroxide (lye) in the city's water supply from 100 parts per million to 11,100 parts per million. Fortunately, a plant employee noticed the change and corrected it. Access to the town's water treatment system was gained through remote access software on the town's computer system that allows "authorized users to access the water treatment system to trouble shoot problems." The hacker accessed the system twice, adjusting the sodium hydroxide setting on the second entry. Afterwards, the remote access software was disabled. The city says that a password is required. The Pinellas County Sheriff's Department initiated an investigation and called in the FBI and the U. S. Secret Service.

Please alert your IT departments and water system operators to examine any remote access software in use. It appears this water treatment facility is using a SCADA system, but the operator corrected the issue before the software detected the manipulation and alarmed due to the unauthorized change. The cyber threat actor likely accessed the system by exploiting cyber security weaknesses including poor password security, an outdated Windows 7 operating system (end of life), and

used the desktop sharing software TeamViewer to remotely gain unauthorized access to the system via Remote Desktop Protocol (RDP) exploits.

The following measures may help protect against this scheme:

- Use multiple factor authentication;
- Use strong passwords to protect RDP credentials;
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured, and secure;
- Audit network configurations and isolate computer systems that cannot be updated;
- Audit the network for systems using RDP, closing unused RDP ports, applying two factor authentication wherever possible, and logging RDP login attempts;
- Audit logs for all remote connection protocols;
- Train users to identify and report attempts at social engineering;
- Identify and suspend access of users exhibiting unusual activity;
- Keep software updated; and
- Discontinue use of Windows 7.

For additional information regarding the Fund's cyber security resources or available cyber coverage, please contact the Fund at www.twcarmf.org.

Sources: Channel 10, Tampa Bay, Florida, website Motherboard, Daily Mail.com

Use the links below for more information and tools

Recent Member Communications

Workers' Compensation Forms

Liability and Property Loss Notices

Fund Contact List

www.twcarmf.org