Water Security Response Information Regarding Advisory: Malicious Actor Compromises U.S. Water Treatment Plant, Changes Chemical Level

Received from EPA 2/10/2021, approved for public dissemination

"The FBI, DHS, US Secret Service, and the Pinellas County Sheriff's Office have issued a joint situational report that concerns the water sector. EPA is providing critical information from this report to the WSCC and GCC for awareness. EPA recommends that all water systems implement the mitigation measures listed at the end of this report where applicable.

Background

On 5 February 2021, unidentified cyber actors obtained unauthorized access, on two separate occasions, approximately five hours apart, to the supervisory control and data acquisition (SCADA) system used at a local municipality's water treatment plant. The unidentified actors accessed the SCADA system's software and altered the amount of sodium hydroxide, a caustic chemical, used as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal.

The unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer, which was installed on one of several computers the water treatment plant personnel used to conduct system status checks and to respond to alarms or any other issues that arose during the water treatment process. All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.

Recommended Mitigation

- Restrict all remote connections to SCADA systems, specifically those that allow physical control and manipulation of devices within the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.
- Install a firewall software/hardware appliance with logging and ensure it is turned on. The firewall should be secluded and not permitted to communicate with unauthorized sources.
- Keep computers, devices, and applications, including SCADA/industrial control systems (ICS) software, patched and up-to-date.
- Use two-factor authentication with strong passwords.
- Only use secure networks and consider installing a virtual private network (VPN).
- Implement an update and patch management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers."

WRF Webinar: Full Lead Service Line Replacement Guidance

The Water Research Foundation is providing a webcast that is free and open to the public. It will feature results and recommendations from WRF Project 4713 "Full Lead Service Line Replacement Guidance," which performed full lead service line (LSL) replacements at over 100 locations across North America. Attendees will learn how to apply lead reduction strategies following full LSL replacement. Utility representatives will share their firsthand experiences and best practices related to LSL replacement.

Date: Tuesday, February 23, 2021

Time: 2:00 – 3:30 p.m., CST

Registration

Operator Certification: Continuing Education Opportunities

To find continuing education opportunities, please view the "Training Calendar" at programs.iowadnr.gov/opcertweb/ Training events where Iowa DNR staff will make presentations are listed below with the presentation name in the description. Also included are training events provided by EPA where Iowa CEU are granted, or events sponsored by Iowa DNR. See the listing on the appropriate date on the Training Calendar for registration instructions. Look at the calendar often, as there are new opportunities posted throughout the week.

- February 16, EPA R7 Module 1 AWIA Workshop, virtual. 1.5 hours CEU, WT or WD. Registration.
- February 17, EPA R7 Module 2 AWIA Workshop, virtual. 1.5 hours CEU, WT or WD. Registration.

- February 18, EPA R7 Module 3 AWIA Workshop, virtual. 1.5 hours CEU, WT or WD. Registration.

A note on Iowa DNR and COVID-19

The Iowa Department of Natural Resources is working with state and local officials to reduce the spread of COVID-19 and has transitioned employees to work remotely. DNR offices are closed to the public during this time and only available by appointment.

In another effort to further reduce the spread of COVID-19, the DNR is encouraging the use of the online services for submitting applications, payments and other daily tasks and interaction with DNR staff.

- Full list of DNR's online services
- Current information on DNR services, facilities and events impacted by COVID-19
- Technical information for regulated businesses in regards to COVID-19

We thank you for your patience and flexibility during this time. If you need to contact DNR staff you can reach them by email or phone or by calling 515-725-8200.