Security Incident at Oldsmar Water Treatment Plant and Lessons Learned

By Patrick Honeycutt, Senior Cybersecurity Architect

LSI listens

BACKGROUND AND OVERVIEW

On February 5, 2021, malicious cyber actor(s) obtained unauthorized remote access to an operator workstation at the Bruce T. Haddock Water Treatment Plant in Oldsmar, FL, which is located about 15 miles northwest of Tampa, FL. According to the Pinellas County Sheriff's office, the unidentified cyber attacker accessed the operator workstation on two (2) separate occasions that day, approximately five (5) hours apart. During the first unlawful intrusion at approximately 8:00 AM, a plant operator observed the mouse cursor moving on the screen of the operator station and assumed that it was probably the supervisor just monitoring the system (because that had occurred in the past). At approximately 1:30 PM, the operator observed someone accessing the computer system again, but that time, various software functions were being opened on the screen, and that continued for approximately 3-5 minutes. Finally, the cyber attacker changed the setpoint for sodium hydroxide (lye) from 100 ppm to 11,100 ppm and then exited the system. The operator saw the change occur and quickly changed the setpoint for sodium hydroxide back to 100 ppm.

After the cyber intrusion, the operator notified his supervisor, and steps were taken to disable the remote access application (i.e., TeamViewer).[1]

POTENTIAL IMPLICATIONS OF THE ATTACK

According to city officials for Oldsmar, it would have taken approximately 24-36 hours for the changes to sodium hydroxide to adversely affect the public water supply, but the system has redundancies built-in to alert them of high pH conditions. Since the plant operator observed the cyber intrusion in progress, the setpoint change was reversed quickly, and Oldsmar's population of 15,000 was never in danger. Additionally, the Industrial Control System (ICS) has been configured with pH alarms that should alert water utility staff of an excessive concentration of sodium hydroxide. The Oldsmar Water Treatment Plant should also have standard operating procedures that should help operators to identify an abnormal pH condition before it affects the public.

Although the city of Oldsmar was never in danger because the unauthorized change was detected quickly, but what could have been the potential implications if the cyber-attack had gone unnoticed? We can look to history to get a glimpse of what might have been possible. In April 2007, personnel at Spencer Water Treatment Plant (located approximately 60 miles west of Boston, MA) added too much lye to their water supply, and it caused over a hundred people to be taken to areas hospitals for treatment and decontamination. The incident at Spencer was the result of internal organizational failures and issues with their notification system, but it involved elevated amounts of sodium hydroxide that affected the public water supply. When sodium hydroxide (lye) is introduced into the water supply in elevated concentrations, it can cause rashes, burns to the body, and other adverse effects.[2] So, in the Spencer incident, the pH "high" alarm sounded, but corrective actions were not taken before the public was adversely affected.

---

1 *Levenson, E. (2021, February 13). Florida water hack highlights risks of remote access work without proper security. Retrieved February 15, 2021, from https://www.cnn.com/2021/02/13/us/florida-hack-remote-access/index.html*

2 *Russell, J. (2007, September 28). State faults Spencer employees in lye water crisis. Retrieved February 15, 2021, from https://www.telegram.com/article/20070928/FRONTPAGENEWS/70928004*

Security Incident at Oldsmar Water Treatment Plant and Lessons Learned

By Patrick Honeycutt, Senior Cybersecurity Architect

LSI listens

LESSONS LEARNED FROM THE OLDSMAR SECURITY INCIDENT

Automation and Process Control

When I first heard about the security incident at Oldsmar, my first thought was that of an Automation and Process Control Engineer and wondered why on earth were setpoint limits not being utilized to restrict the entry of high and low values. Input validation is just a sound practice for configuration and programming, and especially for critical systems. If setpoint limits had been utilized, the cyber attacker would have been unable to easily change the setpoint to a value that is outside of defined limits.

ICS Security Best Practices

In the security incident at Oldsmar, numerous ICS security and industry best practices were not being followed, including but not limited to the following:

- **Remote Access** – For many organizations, remote access capability is critical to facilitate support and troubleshooting efforts, particularly given resource constraints and COVID-19 restrictions. However, remote access should be disabled if it is not required and its use should be otherwise restricted.
- **Multi-Factor Authentication (MFA)** – Remote access from an untrusted network (e.g., Internet, enterprise network, etc.) to trusted ICS devices should have required the use of MFA.
- **Network Segmentation** – Based on the description of the incident, the operator workstation was accessible to the Internet, and remote users were able to connect to it without having to authenticate multiple times. ICS assets should be protected behind a firewall within a dedicated security zone.
- **VPN** – Remote access via an encrypted VPN connection should have been required just to access the Industrial Demilitarized Zone (DMZ), thus utilizing a security appliance to restrict network access and inspect all connections to the ICS environment.
- **Industrial DMZ** – An Industrial DMZ was not utilized to broker connections from an *untrusted* device to the *trusted* ICS operator workstation. All ingress and egress traffic to the ICS environment should go through an Industrial DMZ to facilitate access control, traffic inspection, logging, and monitoring. A Remote Desktop Gateway or jump host should be located in the Industrial DMZ, and it could be utilized to connect to trusted devices within the ICS environment.
- **Principle of Least Privilege** – It is quite possible that the supervisor who uses TeamViewer to check the status of the water system could be provided view-only access to process data for monitoring purposes, thus enforcing the principle of least privilege and least functionality.
- **Data restriction** – ICS data security appears to be inadequate. A unidirectional gateway should be considered for the purpose of sending process data for monitoring purposes. One thing is clear, security zone and network traffic restrictions at the utility are lacking, thus potentially exposing confidential data to security risks.
- **Outdated Operating System** – Although it is unknown if the unsupported version of Windows 7 on the operator station was a factor in the Oldsmar's security breach, it is a known fact that unsupported/unpatched operating systems and 3rd party applications can lead to a wide range of security compromises.
- **Shared user account** – The same user account was shared among multiple employees. Each user of an ICS should be uniquely identified with an individual account for the purpose of role-based access control and accounting. Legacy control systems that do not support individual logons should be migrated when feasible.

- **Password security** – All of the computers shared a single password to access TeamViewer. The best practice recommendation is to create strong passwords and do not share them. A Password Policy should be created to help facilitate the enforcement of password security, and ongoing cyber awareness training should be provided.
- **Host firewall** – A host-based firewall did not appear to be in use.[3] Endpoint security protections must be utilized (e.g., firewall, AV, etc.) and the system should be hardened to remove unnecessary applications and services.
- **Cyber-physical safety system** – It was not disclosed whether Oldsmar's redundancies include a cyber-physical safety system that would bring the system to a safe state in a worst-case scenario (if other control mechanisms had failed). Cyber-physical safety is recommended as a countermeasure to reduce the impact of an ICS security event.[4]
- **Security assessment/audit** – Although the utility stated that they have some redundancies in place to mitigate risk, enabling and using remote access on a system with known security vulnerabilities exposed the organization to a myriad of potential cyber-attacks. A security assessment should be conducted to assess risks and threats to the water treatment plant's ICS environment.

CONCLUSIONS

While there is no "silver bullet" when it comes to ICS Cybersecurity, water utilities and other critical infrastructure sectors can improve their cybersecurity posture by assessing, designing, and implementing security solutions that align with ICS security standards (e.g., NIST 800-82, IEC-62443, etc.) and industry best practices. The strategic use of layered security controls is effective in mitigating security risks, and this approach is also known as "Defense-in-Depth." However, cyber adversaries are continually adjusting their tactics and techniques to evade security controls, so organizations must also constantly refine and adjust their security countermeasures as new threats emerge. Lessons learned from this security incident should serve as a wake-up call for critical infrastructure organizations to evaluate their cybersecurity posture and allocate the necessary funding to make continual improvements because a "set it and forget it" approach is not an effective means of addressing dynamic security threats.

Patrick Honeycutt has over 20 years of cybersecurity and process control experience. He is responsible for overseeing a variety of LSI's cybersecurity endeavors, including ICS/OT cybersecurity assessments against the guidelines and practices of leading security frameworks (NIST 800-82, ISA-99/IEC-62443, etc.), assessment of critical infrastructure against industry-specific federal guidelines (NERC CIP, FERC, CFATS, etc.), and design and implementation of networking and security solutions to align clients' ICS/OT environments with security framework practices and industry-specific federal guidelines. He also helps LSI's customers establish their ICS/OT cybersecurity programs and creates security road maps to help them address cybersecurity risks using a risk-based phased approach. Contact Patrick at 877-735-6905 or phoneycutt@logicalsysinc.com.

LOGICAL SYSTEMS, LLC (LSI) is an outcome-driven systems integrator specializing in process improvement, electrical engineering, automation, systems integration, and manufacturing intelligence (data intelligence, manufacturing execution systems (MES), industrial control system/operational technology (ICS/OT) cybersecurity). LSI employs more than 240 skilled individuals worldwide, with offices in Memphis and Jackson, Tennessee; Golden, Colorado; Rossville, Georgia; Toronto, Ontario; Guangzhou, China; and Taipei, Taiwan.

---

3 *Mass.gov (2021). Cybersecurity Advisory for Public Water Suppliers. Retrieved February 15, 2021, from https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers*

4 *Cybersecurity & Infrastructure Security Agency (2021, February 11). Compromise of U.S. Water Treatment Facility. Retrieved February 15, 2021, from https://us-cert.cisa.gov/ncas/alerts/aa21-042a*