

Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant February 5, 2021



Homeland Security

Science and Technology

WHAT DO WE KNOW ABOUT THE INCIDENT?^{1,2}

- A hacker gained access into the control system of the Oldsmar, Florida water treatment plant on Friday February 5, 2021 and attempted to increase the levels of sodium hydroxide (commonly referred to as lye or caustic soda and used in water treatment to regulate acidity levels, to include reducing lead concentrations in drinking water) in the city's water by adjusting the control setting to more than 100 times its normal levels (100ppm to 11,100ppm or 1.11%).
- The Oldsmar water treatment facility is one of 153,000 facilities³ across the nation and services about 15,000 people.
- The control room uses TeamViewer software⁴ and the plant operator noticed the attempt to remotely increase the sodium hydroxide concentration while in progress. The operator realized that the concentrations were being set to unsafe levels and immediately reduced the control setting back to the appropriate value before the water supply was affected.
- It is unknown but, based on initial S&T modeling data⁵, it is highly unlikely that the increased levels of sodium hydroxide in the water at the Oldsmar, FL facility would have led to any public health impact, even if not interdicted.
- The city has taken steps to prevent further access into the system by disabling the remote-access system and ensuring other safeguards are in place⁶.
- A joint investigation by the Pinellas County Sheriff's Office, FBI and Secret Service is ongoing, and it is unknown if the breach was domestic or foreign.
- Sen. Marco Rubio (FL) tweeted that he wants this incident treated as a matter of national security.

WHAT ARE THE POTENTIAL IMPACTS OF THE INCIDENT?

- This specific incident did not result in any public health impacts, however the attack highlights potential vulnerabilities for systems that use networked industrial control systems and outdated operating systems.
- This incident may inspire similar attacks seeking to exploit such vulnerabilities at municipal water treatment plants or food suppliers that use water sourced on-site.
- Tampering with water treatment chemicals, by either increasing or decreasing the concentration delivered, could cause public health impacts.

WHAT IF THERE WAS A HIGH LEVEL OF SODIUM HYDROXIDE IN DRINKING WATER?

- A sodium hydroxide level in water at a high concentration, such as that found in liquid drain cleaner, can cause chemical burns to skin, eyes, mouth, throat, esophagus, and stomach through ingestion or dermal exposure, such as showering⁷.
- Swallowing a caustic solution of sodium hydroxide may also cause vomiting, nausea and diarrhea. Damage may last for several weeks after ingestion, and death may occur as long as a month later⁸.
- The presence of sodium hydroxide in high concentrations may impart a smell or taste, although the ability to notice a change will vary from person to person.



Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant February 5, 2021



Homeland Security

Science and Technology

ONGOING ACTIONS

- Use the CAPT web capability to simulate water system chemical attacks using different chemicals as surrogates to provide awareness of the potential harm.
- Compile a detailed bulletin on these type of chemical events to be shared with the HSE.
- Coordinate with DHS CISA and CWMD to outreach to American Water Works Association (AWWA) and other water sector industry partners.
- Coordinate with DHS CISA and CWMD to outreach to food defense industry partners.

WHAT ARE THE INFORMATION/DATA GAPS?

- All possible chemicals deployed at wastewater and drinking water sites.
- Other chemicals and related infrastructure that are controlled by similar systems.
- Baseline flowrate of water to be treated and flowrate of sodium hydroxide addition. Maximum contents and the concentration of the sodium hydroxide in chemical addition tanks.
- Locations of downstream pH instrumentation and Quality Control/Quality Assurance procedures.
- Demographics of vulnerabilities for different sized water treatment systems across the U.S.

OTHER CONSIDERATIONS

WATER TREATMENT CHEMICALS OF CONCERN⁹

- Acids (nitric and sulfuric) and bases (potassium hydroxide, calcium oxide and calcium hydroxide) used for pH control
- Coagulating chemicals for pollutant removal such as aluminum and iron salts
- Fluoride compounds

- Disinfection chemicals such as chlorine, chlorine dioxide, chloramine, ozone and ammonia
- Odor and taste control such as activated carbon, potassium permanganate
- Corrosion control with blended phosphates

OTHER POTENTIAL WATER SYSTEM ATTACKS

- Direct introduction of toxic chemicals into building supply line which then can potentially contaminate the main water system (Back flushing).
- Similar attacks could also impact food, chemical, healthcare, pharmaceuticals, and other Supervisory Control and Data Acquisition (SCADA) controlled infrastructure.

HISTORICAL INCIDENTS

- In 2020, there were multiple attempted cyberattacks on Israeli water supplies all were averted.¹⁰
- 2019 a water utility in Illinois was hacked in a cyberattack traced back to Russia. The attackers manipulated a water pump repeatedly, eventually damaging it.¹¹
- In 2016, hackers breached an unnamed water utility and manipulated systems for water treatment and flow control.^{12,13}
- In 2000, the first known cyberattack on an industrial control system, the Marochy Shire wastewater attack, in Queensland, Australia, resulted in 800,000 liters of raw sewage spilling out into local parks, rivers and other locations.¹⁴
- In 1979, a manually operated valve was “inadvertently left open” overnight and caused the fluoride concentrations of the Annapolis water supply to be 15 times its usual level contributing to the death of a 65 year-old man.^{15, 16}



Chemical Considerations for the Incident at Oldsmar, Florida Water Treatment Plant February 5, 2021



Homeland Security

Science and Technology

References

- (1) <https://www.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html>, accessed 2/9/2021.
- (2) <https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/>, accessed 2/9/2021.
- (3) <https://www.cisa.gov/water-and-wastewater-systems-sector>, accessed 2/9/2021.
- (4) <https://www.darkreading.com/attacks-breaches/florida-water-utility-hack-highlights-risks-to-critical-infrastructure/d/d-id/1340112>, accessed 2/9/2021.
- (5) DHS S&T CSAC preliminary CAPT Web modeling assessment.
- (6) <https://abc7ny.com/city-of-oldsmar-water-hack-sodium-hydroxide-news-lye-drain-opener/10322199/>, accessed 2/9/2021.
- (7) Safety Data Sheet, Sigma-Aldrich, Sodium Hydroxide, Version 6.6, Revision date 01/15/2020.
- (8) University of Florida Health, sodium hydroxide poisoning, <https://ufhealth.org/sodium-hydroxide-poisoning>, accessed 2/9/2021.
- (9) PA Department of Environmental Protection; Drinking Water Operator Certification Training; Module 21: Chemical Addition; March 2017.
- (10) <https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-water-infrastructure.html>, accessed 2/9/2021.
- (11) <https://wsabc.ca/water-utility-hacked-are-our-scada-systems-at-risk/>, accessed 2/9/2021.
- (12) <https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/>, accessed 2/9/2021.
- (13) <https://securityaffairs.co/wordpress/45550/hacking/cyber-attacks-waterr-utility.html>, accessed 2/9/2021.
- (14) https://www.mitre.org/sites/default/files/pdf/08_1145.pdf, accessed 2/9/2021.
- (15) <https://www.washingtonpost.com/archive/politics/1979/11/29/fluoride-ruled-a-cause-in-death/51a48e52-6ed2-4926-9b22-9ddc0ccedc8b/>, accessed 2/9/2021.
- (16) <https://www.newspapers.com/clip/7948856/1979-nov-29death-linked-to-annapolis/>, accessed 2/9/2021.

