# Oldsmar Water Treatment Attack

## Remote access intrusion targeting public water supply

OT Security Learning Series

Document 415 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

# Contents

# 1 Introduction

In February 2021, an attacker remotely accessed the water treatment plant in Oldsmar, Florida, and attempted to increase sodium hydroxide (lye) levels from 100 parts per million to 11,100 ppm—a potentially lethal concentration. An alert operator observed the intrusion in real-time and immediately reversed the changes.

**Critical**

This attack demonstrated that small water utilities are vulnerable targets. The attacker used legitimate remote access software (TeamViewer) to directly manipulate chemical dosing—a direct threat to public health.

## 1.1 Key Facts

| Attribute | Details |
|---|---|
| Date | February 5, 2021 |
| Target | Oldsmar Water Treatment Plant, Florida |
| Population Served | Approximately 15,000 residents |
| Attack Vector | TeamViewer remote access software |
| Attack Method | Increased sodium hydroxide (NaOH) setpoint |
| Change Attempted | 100 ppm to 11,100 ppm (111x increase) |
| Detection | Operator observed cursor movement in real-time |
| Impact | None—attack reversed immediately |
| Attribution | Initially unknown; later linked to former employee |

# 2 Attack Details

## 2.1 Attack Timeline

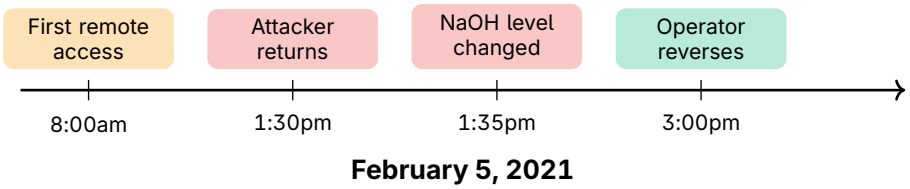


Figure 1: Oldsmar Attack Timeline

- **8:00 AM:** First brief remote access—operator noticed but assumed supervisor checking in
- **1:30 PM:** Attacker returns via TeamViewer
- **1:30–1:35 PM:** Attacker navigates SCADA interface, changes NaOH from 100 to 11,100 ppm
- **1:35 PM:** Operator observes changes and immediately reverses them

- **3:00 PM:** Plant supervisor notified, law enforcement contacted

### 2.2 Attack Method

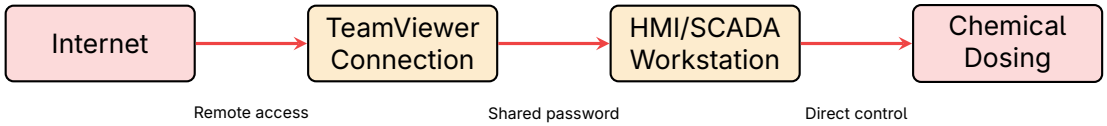


Figure 2: Oldsmar Attack Path

**Warning**

**Critical Security Failures:**

- TeamViewer installed directly on SCADA workstation
- Shared password among all plant staff
- No multi-factor authentication
- Windows 7 (end-of-life operating system)
- No network segmentation between IT and OT

## 3 Sodium Hydroxide Danger

**Critical**

**Sodium Hydroxide (Lye/Caustic Soda):**

- Normal use in water treatment: pH adjustment, corrosion control
- Safe level: 25–100 ppm for treatment purposes
- Attempted level: 11,100 ppm (extremely dangerous)
- Effects: Chemical burns, tissue damage, potentially fatal if ingested

### 3.1 Safety Barriers

While the attack was caught immediately, multiple safety barriers would have prevented harm:

| Barrier | Protection |
|---|---|
| Operator monitoring | Real-time observation caught the change |
| pH sensors | Would detect abnormal levels |
| Time delay | Changes take 24+ hours to reach customers |
| Residual monitoring | Downstream sensors check water quality |
| Manual sampling | Regular testing would detect anomalies |

Table 1: Defense-in-Depth Safety Barriers

**Information**

Defense-in-depth means no single failure causes harm. Even if the cyber attack succeeded, multiple process and safety controls would likely have prevented contaminated water from reaching customers.

# 4 Security Failures Analysis

## 4.1 Remote Access Issues

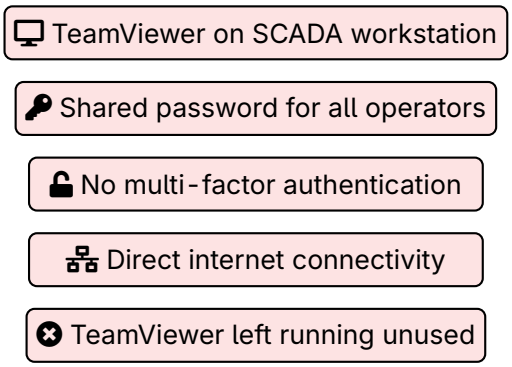


Figure 3: Remote Access Security Failures

## 4.2 System Configuration Issues

- **Outdated OS:** Windows 7 past end-of-life (no security updates)
- **Flat network:** No segmentation between business and OT systems
- **No firewall:** Direct internet access to SCADA
- **Shared credentials:** No individual accountability
- **No logging/alerting:** Remote access not monitored

# 5 Investigation Findings

## 5.1 Initial Response

Investigations involved:

- FBI (federal investigation)
- Pinellas County Sheriff's Office
- CISA (technical assistance)
- Secret Service (critical infrastructure)

### 5.2 Attribution Challenges

Initial attribution was difficult because:

- Shared credentials meant no individual identification
- TeamViewer logs insufficient for definitive attribution
- Remote access could originate from anywhere
- Multiple parties knew the shared password

**Information**

In late 2023, a former Oldsmar employee was charged in connection with the attack. The case highlights how insider threats and weak access controls combine to create serious risks.

## 6 Lessons Learned

### 6.1 Immediate Recommendations

**Key Point**

**Critical actions for water utilities:**

1. **Remove or secure remote access:** No direct internet-to-SCADA connections
2. **Implement MFA:** Required for all remote access
3. **Individual accounts:** No shared passwords
4. **Update operating systems:** Replace Windows 7 and other EOL systems
5. **Network segmentation:** Separate IT, OT, and internet
6. **Monitor remote access:** Log and alert on connections

### 6.2 Secure Remote Access Architecture

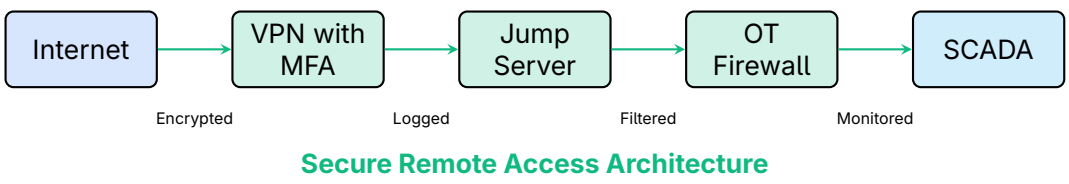


Figure 4: Recommended Secure Remote Access

### 6.3 Water Sector Specific Guidance

- Review CISA/EPA water sector guidance
- Participate in WaterISAC threat sharing
- Conduct regular security assessments

- Train operators on security awareness
- Develop incident response procedures

# 7 Broader Implications

## 7.1 Small Utility Challenges

**Warning**

Small water utilities face unique challenges:
- Limited IT/security staff and expertise
- Budget constraints for security improvements
- Legacy systems difficult to upgrade
- Remote operations require remote access
- Thousands of potential targets nationwide

## 7.2 Regulatory Response

The Oldsmar incident prompted:

- **CISA alerts:** Guidance for water and wastewater utilities
- **EPA focus:** Increased attention on water sector cybersecurity
- **State actions:** Florida increased water utility oversight
- **WaterISAC:** Enhanced threat sharing and resources

# 8 Summary

**Key Takeaways**

- **Direct OT manipulation:** Attacker changed chemical dosing in real-time
- **Remote access risk:** TeamViewer on SCADA without MFA
- **Shared credentials:** No accountability or traceability
- **Operator saved the day:** Human vigilance caught the attack
- **Defense-in-depth works:** Multiple barriers would have prevented harm
- **Small utilities at risk:** Limited resources, high vulnerability

# 9 Further Reading

### Official Advisories

- **CISA** – Compromise of U.S. Water Treatment Facility
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a
- **FBI/CISA/EPA** – Water Sector Cybersecurity Brief
  https://www.cisa.gov/resources-tools/resources/water-and-wastewater-cybersecurity

### Resources

- **WaterISAC** – Water Information Sharing and Analysis Center
  https://www.waterisac.org/
- **EPA** – Water Sector Cybersecurity Resources
  https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
- **AWWA** – Cybersecurity Guidance
  https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance