(TLP:CLEAR) Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (Updated November 30, 2023) - WaterISAC

By jlwalker

Published: 2023-11-30 · Archived: 2026-04-05 19:50:38 UTC

As WaterISAC continues to monitor for more information regarding this incident, we would like to make members aware that this may not be an isolated incident. There have been a few open source reports about additional incidents with similar characteristics having occurred at other US water and wastewater utilities. WaterISAC is currently attempting to confirm those reports.

Based on this information, as a reminder members are highly encouraged to:

- **Check for Unitroincs PLCs in your environment,** especially ones directly exposed to the internet which are trivial to discover through a basic internet (Shodan, Censys, etc.) search. *As a generally recommended practice, it is important to identify any PLC in your environment that might be directly connected to the internet or other untrusted network – not just the ones identified in this current incident.*
- **Change default passwords.** Per the previously shared CISA Alert Tuesday evening, it is believed the threat actors are leveraging default passwords that have not been changed after deployment to gain access to impacted devices. *Again, as a generally recommended practice, this should be performed on every device or component active in your networks (OT or IT).*
- **Refrain from connecting (all) PLCs to the internet.** If remote access is not necessary, a PLC connected to the internet represents an unnecessary risk to safety, availability, and control of your SCADA environment.
    - However, **if remote access is absolutely necessary**, it is important that at a minimum, it securely sits behind a firewall and requires a VPN to access.
    - Additionally, **MFA should be implemented**, at the very least on the VPN (if the PLC doesn't support MFA).
- If you haven't already, **review the CISA Alert**, Exploitation of Unitronics PLCs used in Water and Wastewater Systems for more details and **address accordingly**.

Important: For utilities that outsource SCADA support, please **consult with integrators/support vendors to confirm/insist that recommended practices are being followed**. Internet exposed PLCs are exceedingly trivial to discover and default passwords are widely known by attackers, making them easy to gain access to.

Please discourage "*this won't happen to us*" notions. Often, we aren't targets for who/where we are, but for what we have (data or components) and how accessible (vulnerable/exploitable) it is – *regardless of the size of our organization or how many people we service.*

November 27, 2023

While few details are currently known, according to open-source reporting, on Saturday the **Municipal Water Authority of Aliquippa** in western Pennsylvania was **attacked by an Iranian-backed cyber group known as CyberAv3ngers**. The authority reported the actors were able to gain control of a remote booster station serving two townships, but stressed there is no known risk to the drinking water or water supply. CyberAv3ngers claims to be an active group focused on targeting Israeli water and energy sites – including ten water treatment stations in Israel as of Oct. 30, 2023, according to their X page. The Pennsylvania State Police is currently investigating.

A local Pittsburgh news channel (KDKA) reported that CyberAv3ngers took control of the booster station that monitors and regulates pressure for Raccoon and Potter Townships. An alarm reportedly went off as soon as the attack occurred. The system has been disabled and is being operated manually. The compromised device is reported to be a Unitronics.

Of note, the news site has posted an image stating it was submitted by the water authority. The image suggests the attacker's message is displayed on the system that was compromised with the Unitronics device and model (V570). While there's generally nothing wrong with providing attackers messages to the media, perhaps better operational security should be maintained by cropping the image to omit the device and model or other key data.

WaterISAC will be monitoring this situation for updated information and will advise of any significant developments.

Incident Reporting

If your utility experiences any cyber incidents or suspicious activity, contact the FBI via your local Field Office, Cyber Watch (CyWatch) at (855) 292-3937 or Cy*****@*bi.gov, or the Internet Crime Complaint Center (IC3). You can also contact CISA at re****@**sa.gov or (888) 282-0870. Additionally, WaterISAC encourages members to share information by emailing an*****@*******ac.org, calling 866-H2O-ISAC, or using the online incident reporting form.

To help prevent incidents, WaterISAC encourages water and wastewater utilities to sign up for CISA's free Cyber Vulnerability Scanning (VS) service. The VS service continuously assesses the health of internet-accessible assets by checking for known vulnerabilities, weak configurations – or configuration errors – and suboptimal security practices. CISA created a fact sheet on the VS service focused on water and wastewater utilities, available here. WaterISAC also hosted a briefing on the VS service with CISA personnel on September 28 – the recording and presentation are posted on WaterISAC's website here (only WaterISAC members can access the webpage).

Marked TLP:CLEAR, recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, or TLP, visit CISA.
