Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA

Published: 2023-11-28 · Archived: 2026-04-05 15:53:18 UTC

CISA is responding to active exploitation of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) Sector. Cyber threat actors are targeting PLCs associated with WWS facilities, including an identified Unitronics PLC, at a U.S. water facility. In response, the affected municipality's water authority immediately took the system offline and switched to manual operations—there is no known risk to the municipality's drinking water or water supply.

WWS Sector facilities use PLCs to control and monitor various stages and processes of water and wastewater treatment, including turning on and off pumps at a pump station to fill tanks and reservoirs, flow pacing chemicals to meet regulations, gathering compliance data for monthly regulation reports, and announcing critical alarms to operations.

Attempts to compromise WWS integrity via unauthorized access threaten the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

The cyber threat actors likely accessed the affected device—a Unitronics Vision Series PLC with a Human Machine Interface (HMI)—by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet. To secure WWS facilities against this threat, CISA urges organizations to:

- Change all default passwords on PLCs and HMIs and use a strong password. Ensure the Unitronics PLC default password "1111" is not in use.
- Require multifactor authentication for all remote access to the OT network, including from the IT network and external networks.
- Disconnect the PLC from the open internet. If remote access is necessary, control network access to the PLC.
    - Implement a Firewall/VPN in front of the PLC to control network access to the remote PLC. A VPN or gateway device can enable multifactor authentication for remote access even if the PLC does not support multifactor authentication. Unitronics also has a secure cellular based longhaul transport device that is secure to their cloud services.
    - Use an allowlist of IPs for access.
- Back up the logic and configurations on any Unitronics PLCs to enable fast recovery. Become familiar with the process for factory resetting and deploying configurations to a device in the event of being hit by ransomware.
- If possible, utilize a TCP port that is different than the default port TCP 20256. Cyber actors are actively targeting TCP 20256 after identifying it through network probing as a port associated to Unitronics PLC. Once identified, they leverage scripts specific to PCOM/TCP to query and validate the system, allowing for further probing and connection. If available, use PCOM/TCP filters to parse out the packets.
- **Updated Dec. 19, 2023:**

- Update PLC/HMI to the latest version provided by Unitronics.
- See Unitronics Cybersecurity Advisory 2023-001 for more information.
- See joint Cybersecurity Advisory, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (published Dec. 1, 2023) for additional technical information and mitigations.
- See CISA's Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords.

CISA and WWS Sector partners have developed numerous tools and resources that water utilities can use to increase their cybersecurity. Please visit:

- CISA: Water and Wastewater Cybersecurity
- EPA: Cybersecurity for the Water Sector
- WaterISAC: Resource Center
- American Water Works Association: Cybersecurity and Guidance

Report

Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or by calling 1-844-Say-CISA (1-844-729-2472), or your local FBI field office.
