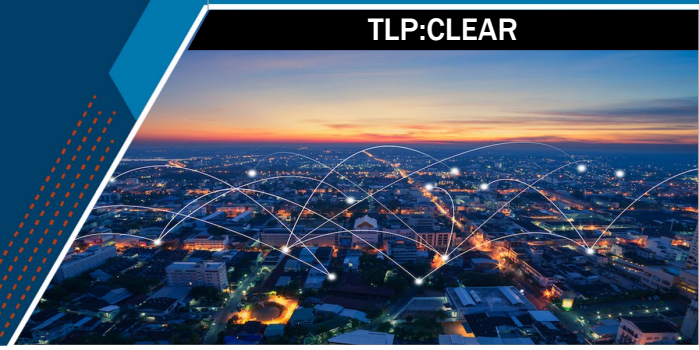
Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems



Overview

The Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) often identify internet-exposed Human Machine Interfaces (HMIs) through scanning via publicly available web-based search platforms. HMIs enable operational technology (OT) owners and operators to read Supervisory Control and Data Acquisition (SCADA) systems connected to programmable logic controllers (PLCs). In the absence of cybersecurity controls, unauthorized users can exploit exposed HMIs in Water and Wastewater Systems to:

- View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings) and
- Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process.

Threat actors have demonstrated the capability to find and exploit internet-exposed HMIs with cybersecurity weaknesses easily. For example, in 2024, pro-Russia hacktivists manipulated HMIs at Water and Wastewater Systems, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts at water systems and forced victims to revert to manual operations. (For more information, see the joint fact sheet Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity.)

EPA and CISA are releasing this fact sheet to provide Water and Wastewater Systems with recommendations for limiting the exposure of HMIs on the internet and securing them against malicious cyber activity.

Mitigations

EPA and CISA strongly encourage Water and Wastewater Systems to implement the following mitigations to harden remote access to HMIs. Organizations may need to consult with their system integrators and request the implementation of these mitigations.

- Conduct an inventory of all internet-exposed devices.
- If possible, disconnect HMIs and all other accessible and unprotected systems from the public-facing internet.
- If it is not possible to disconnect the device, secure it by creating a username and strong password to prevent a threat actor from easily viewing and accessing the devices. Change factory default passwords.

- Implement a strong password and multifactor authentication (MFA) for all access to the HMI and OT network.
- Implement network segmentation by enabling a demilitarized zone (DMZ) or a bastion host at the OT network boundary.[1]
- Implement geo-fencing across the entire network and enforce network segmentation based on specific locations.
- Keep all systems and software up to date with patches and necessary security updates.
- Establish an allowlist that permits only authorized IP addresses to access the devices.
- Log remote logins to HMIs; be aware of failed attempts and unusual times.
- Implement your vendor's recommendations for best securing your product.
- Sign up for CISA's free cybersecurity vulnerability scanning service to identify software vulnerabilities and confirm that patching is up to date and done correctly.

Resources

CISA's Free Cyber Vulnerability Scanning for Water Utilities can assist water utilities assess and monitor internet-accessible assets and evaluate vulnerabilities within those assets. Email vulnerability@cisa.dhs.gov to request services. **Note:** Clicking on the email link will open a dialog box with the subject line "Requesting Vulnerability Scanning Services" preformatted for ease. Include the name of your utility, a point of contact with an email address, and the physical address of your utility's headquarters.

Joint fact sheet Top Cyber Actions for Securing Water Systems provides actions Water and Wastewater Systems can take to reduce risk to and improve resilience against malicious cyber activity and provides free services, resources, and tools to support these actions.

EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems assists owners and operators of drinking water and wastewater systems with assessing gaps in their current cybersecurity practices and controls and identifying actions that may reduce their risk from cyberattacks. The document also provides information on receiving technical assistance, cybersecurity training, and cybersecurity funding.

CISA's Stuff Off Search provides guidance for identifying internet-exposed assets.

Water systems requiring additional support for implementing any of the aforementioned mitigations should contact their regional CISA Cybersecurity Advisor and/or EPA for assistance.

For guidance on OT remote access, see NIST TN 2283 (Initial Public Draft): Cybersecurity for the Water and Wastewater Sector: Build Architecture. Operational Technology Remote Access.

[1] An OT DMZ makes it more difficult for an unauthorized user to reach private networks and prevents malicious actors from performing reconnaissance to search for potential targets on the OT network. A DMZ may include a proxy server, which centralizes internal traffic flow and simplifies monitoring and recording of that traffic. A bastion host is a specialized, highly secured system, often a server or dedicated workstation, that serves as the sole access point between an external network (such as the internet or internal IT network) and a protected internal network.