

PROTECTING AGAINST CYBERATTACKS



Water and wastewater facilities run on connected systems, and weather monitoring equipment is often part of that network.

Cyberattacks: A Growing Threat

Over the past few months, hackers have attacked municipal water systems across the country, targeting the programmable logic controllers (PLCs), that run pumps and valves controlling water flow.¹

Weather monitoring equipment often sits on these same industrial networks, connected to the PLCs and SCADA systems these advisories are warning about.

In August, the NSA, CISA, FBI, Department of Energy, and EPA issued a joint advisory about a related threat targeting equipment common across water, wastewater, energy, and manufacturing facilities.² The advisory found attackers scanning the internet for systems that are exposed online, running outdated software, or still using default passwords. As the agencies put it plainly: this isn't a theoretical risk, it's an active one.

While we are not aware of any attacks involving our equipment, CWS president Nader Khoury provides some tips on how to keep your weather station secure, so that it does not become a system vulnerability.

How These Break-Ins Happen

Hackers generally aren't breaking through sophisticated defenses. They're finding equipment that was left exposed, whether through a weak password, outdated firmware, or a remote connection nobody locked down properly.

Vulnerable equipment gets identified through internet scans that look for anything connected directly online. Attackers try default or previously leaked passwords, or take advantage of outdated firmware. Sometimes



Weather MicroServer installed alongside PLCs at a wastewater treatment facility, the same type of industrial network environment hackers have been targeting.

the opening comes through a remote access connection that was set up for convenience and never properly secured, including one set up by a third-party vendor.

Utilities Are Already Investing in Fixes

Water and wastewater managers aren't standing still on this. The EPA has announced \$11.75 million in grants to help drinking water systems strengthen cybersecurity and resilience, including funding for San Diego to replace vulnerable PLCs.³ It's a sign the industry is taking this seriously, and a good moment for anyone managing connected equipment to do the same. Weather station sensors may be connected to the monitoring systems via 4-20 mA analog interface which is a secure connection. Alternatively, many water systems utilize CWS's Weather MicroServer for industrial interfaces.

How to Secure Your Weather MicroServer

A proper configuration already avoids nearly every one of the pitfalls mentioned above. The Weather MicroServer connects to a network over a single Ethernet cable, and its ports and interfaces are hardened to minimize the risk of a security breach.⁴ CWS president Nader Khoury offers the following reminders:

1. Change the default Admin password.
2. Install the Weather MicroServer behind a properly configured firewall.
3. Keep the MicroServer updated to the latest available firmware version (currently 4.4.16167).
4. Do not make the Weather MicroServer available via remote access.
5. If weather data is needed over the internet, take advantage of our CWS Cloud Weather Server. The MicroServer is able to upload data to the Cloud Weather Server over secure HTTPS protocol.
6. When remote access is necessary, communications should be routed through a secure gateway or VPN with multiple levels of authentication, with limited user access.
7. If connecting the weather station to a local area network is prohibited in your organization, we offer our weather stations (such as the Orion 420™) with analog (4-20mA or 0-5V) interfaces to programmable logic controllers.
8. We also offer stand-alone systems with Display Consoles or serial connection to computers that are not on the network, running WeatherMaster™ software independently.

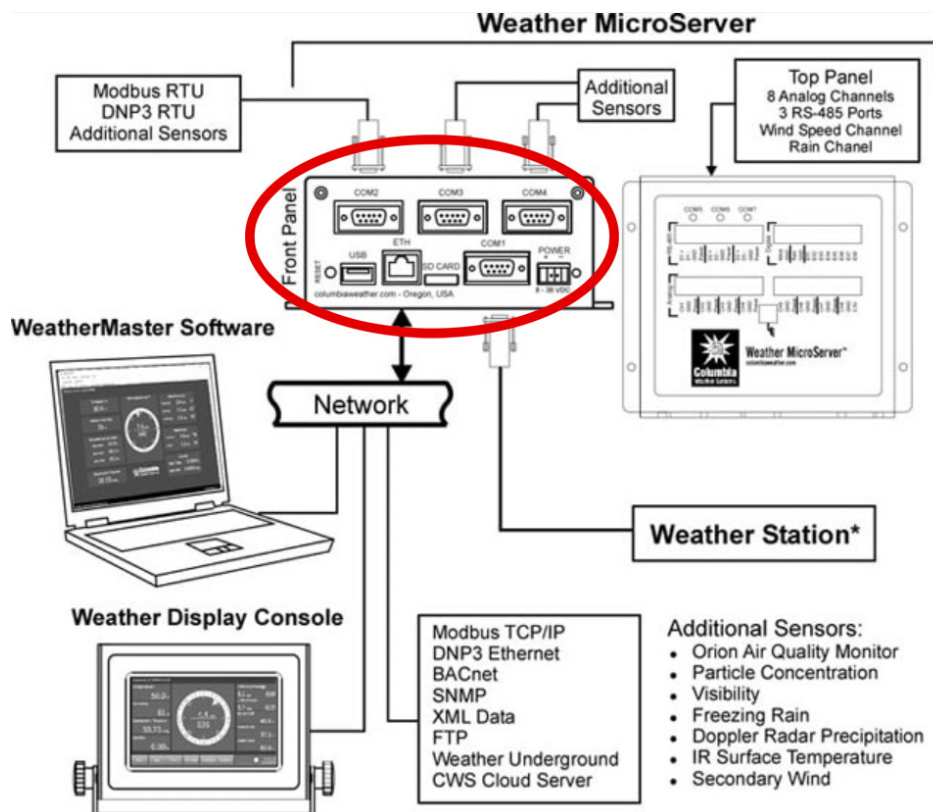
What a Properly Secured System Looks Like

The diagram below shows a typical Weather MicroServer setup. The MicroServer, circled, is the component this guidance focuses on: sensors connect to the system through the interface module, and it communicates outward using protocols such as Modbus, DNP3, BACnet, SNMP, FTP, and our own Cloud Server.



The Weather MicroServer is a data logger and powerful communication device. It includes a web browser user interface with real-time dashboards, configuration, and data export.

This is the same category of equipment named in the recent advisories: industrial hardware that reports real-time data, sometimes over a network.² The difference is in how it's set up. When a system is placed behind a firewall, kept off direct remote access, and connected to the internet only through our encrypted Cloud Weather Server, it no longer matches the profile these cyberattacks were designed to exploit.



The Fix is Simple

The reassuring part is that the fix rarely requires anything complicated. Changing a default password, keeping firmware current, and being thoughtful about remote access, these actions close off almost every entry point of attack.

Our job is to make weather monitoring easy -- and secure -- so you can do your job better.

Contact us to learn how we can help you set up your weather monitoring system securely.

Call or email for a quote | 503-629-0887 | info@columbiaweather.com

References and Citations

1. Akoto, W. (2026, August 5). How hackers attack municipal water systems — and why the utilities are so vulnerable. TPO Magazine. https://www.tpomag.com/online_exclusives/2026/08/how-hackers-attack-municipal-water-systems
2. Wastewater Digest. (2026, August 25). Federal agencies warn of active cyber threat to Siemens PLCs. Wastewater Digest. <https://www.wwdmag.com/utility-management/news/55400547/federal-agencies-warn-of-active-cyber-threat-to-siemens-plcs>
3. WaterWorld. (2026, September 1). EPA grants target cybersecurity, extreme weather risks at water systems. WaterWorld. <https://www.waterworld.com/water-utility-management/news/55402120/epa-grants-target-cybersecurity-extreme-weather-risks-at-water-systems>
4. Columbia Weather Systems. (n.d.). Will a weather station impact network security? <https://columbiaweather.com/resources/network-security/>