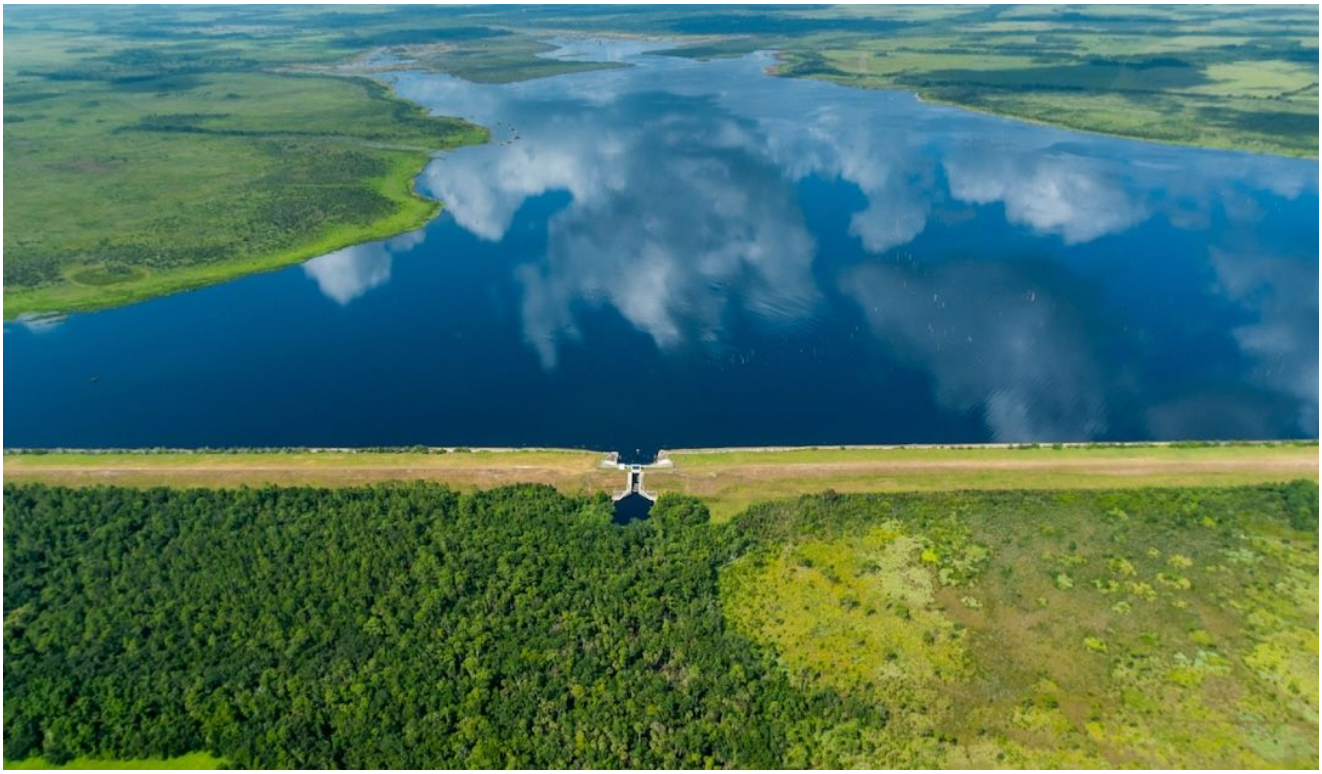
Florida water agency latest to confirm cyber incident as feds warn of nation-state attacks

therecord.media/florida-water-agency-ransomware-cisa-warning-utilities



The Upper St. Johns River Basin Project in Florida. Image: St. Johns River Water Management District / Facebook

Jonathan Greig

December 4th, 2023

A regulatory agency in Florida that oversees the long-term supply of drinking water confirmed that it responded to a cyberattack over the last week as the top cybersecurity agencies in the U.S. warned of foreign attacks on water utilities.

A spokesperson for the St. Johns River Water Management District, which works closely with utilities on water supply issues, confirmed that it “identified suspicious activity in its information technology environment” and that “containment measures have been successfully implemented.”

The agency does not have direct control over water utility technology.

On Friday, a ransomware gang said it attacked the organization, providing samples of what it stole. The cybercriminals did not say how much total data was taken in the attack.

Most of the work by the St. Johns River Water Management District is centered around educating the public about water conservation, setting rules for water use, conducting research, collecting data, restoring and protecting water above and below the ground, and preserving natural areas.

“The District is actively monitoring its IT networks to ensure there is no ongoing, malicious persistence,” the agency spokesperson said. “Accordingly, the District is continuing its normal business operations. Until our investigation is complete, we are unable to comment further.”

IRGC attacks on Unitronics

The attack comes after U.S. officials raised alarms last week about several incidents involving companies involved in water treatment and distribution.

The Cybersecurity and Infrastructure Security Agency (CISA) said it is responding to the active exploitation of Unitronics programmable logic controllers (PLCs) used by many organizations in the water sector.

CISA linked the advisory to a notice from the Water Information Sharing and Analysis Center (WaterISAC) about an attack on a water utility in Pennsylvania reported November 26.

Another water utility serving 2 million people in North Texas said Tuesday that it is also dealing with a cybersecurity incident that caused operational issues, but officials did not say if it was related to issues with Unitronics PLCs.

CNN reported late last week that CISA told Senate and House staffers on Thursday that “less than 10” water facilities in different parts of the US have faced cyberattacks in recent days.

The hackers behind the incident in Pennsylvania have filled their social media feed with references to the leaders of Iran and have pledged to attack any entities with products or ties to Israel — already touting attacks on 10 water treatment plants in Israel.

By Friday, CISA worked with the FBI, National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD) to release an advisory warning that hackers — who go by the name CyberAv3ngers — are connected to the Iranian government’s Islamic Revolutionary Guard Corps (IRGC).

The group is “actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs),” the advisory says.

The agencies said hackers affiliated with the IRGC have compromised default credentials in Unitronics devices since at least November 22 and explicitly claim that their motivation is to target anything associated with Israel, according to defacement images seen by U.S.

authorities.

The kind of Unitronics devices being attacked are often exposed to the internet due to the remote nature of their control and monitoring functionalities, they explained.

> At least 539 Unitronics PLC instances (port 20256/tcp) still publicly exposed worldwide (2023-12-02 scan). Unitronics PLC instances have been targeted recently as part of attacks against Water & Wastewater systems. (see @CISACyber @WaterISAC alert: https://t.co/OywIVYxo8o) pic.twitter.com/XgYrRZbfBm
>
> — Shadowserver (@Shadowserver) December 3, 2023

“The compromise is centered around defacing the controller’s user interface and may render the PLC inoperative. With this type of access, deeper device and network level accesses are available and could render additional, more profound cyber physical effects on processes and equipment,” they said.

While the U.S. campaign began in November, the hackers have been active since at least September, claiming on their Telegram channel both legitimate and false attacks against Israeli PLCs in the water, energy, shipping, and distribution sectors.

Cybersecurity nonprofit Shadowserver Foundation said that through its research tool, they found at least 539 Unitronics PLC instances still publicly exposed worldwide.

- Industry
- News
- Cybercrime

No previous article

No new articles

Jonathan Greig

Jonathan Greig is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.