

Attacks on US Critical Infrastructure

Over the weekend of July 26 and 27, 2026, more than 30 public water systems across Minnesota were hit in a coordinated cyberattack, one of the largest on local water infrastructure in the state's history. At least one plant was knocked offline and other communities were forced onto manual operation. Investigators have tentatively linked the attack to Iran, and researchers have pointed to the Iranian state-directed group CyberAv3ngers.

It came just four days after a July 22 update from CISA expanding the scope of the April 7 joint advisory on Iranian-affiliated actors, which we shared with you earlier this year. The attackers are believed to have exploited a known flaw in the facilities' industrial controllers, one the manufacturer has confirmed has no patch available. Small organizations make attractive targets because many lack dedicated security resources, and in some cases the equipment is left exposed to the internet or managed through remote-access tools.

With Iranian-affiliated groups favoring targets that are behind on security fundamentals and moving quickly to exploit newly published vulnerabilities, prompt patching, restricted remote access, and modern monitoring and detection can help keep your organization off the list of easy targets.

If you would like Sandbox Technologies to review your environment or discuss your current security posture in light of this attack, please respond to this email to reach me directly. We will review your environment and advise you on next steps.

Further information is available via the links provided below.

CISA Advisory AA26-097A: Iranian-Affiliated Cyber Actors Exploit PLCs Across US Critical Infrastructure

Cybernews: Iranian Hackers Hit 30 Minnesota Water Systems

The Register: Iran-Linked CyberAv3ngers Suspected in Attacks on Minnesota Water Systems

Tenable: Coordinated Cyberattack on Minnesota Water Utilities, What You Need to Know

Ref. Iranian-Linked Cyberattack on Minnesota Water Systems, July 2026

Sincerely,

Chris Harper

Chief Security Officer

Sandbox Technologies, Inc.