Unpatched Security Flaws Expose Water Pump Controllers to Remote Hacker Attacks

A water pumping system made by ProPump and Controls is affected by several vulnerabilities that could allow hackers to cause significant problems.

The impacted product is the Osprey Pump Controller made by US-based ProPump and Controls, a company that specializes in pumping systems and automated controls for a wide range of applications, including golf courses and turf irrigation, municipal water and sewer, biogas, agricultural, and industrial.

The vulnerabilities were discovered by Gjoko Krstic, founder and chief information security engineer of Macedonian cybersecurity research firm Zero Science Lab. The security holes were identified during an assessment at a client that involved the analysis of actual devices – rather than just firmware image analysis, as is often the case with industrial control system (ICS) research.

Krstic attempted to report his findings to the vendor directly, as well as through the US Cybersecurity and Infrastructure Security Agency (CISA) and Carnegie Mellon University's Vulnerability Information and Coordination Environment (VINCE). However, the vendor has not responded and the vulnerabilities likely remain unpatched.

SecurityWeek reached out to ProPump and Controls for comment 48 hours before this article was published, but the company has not responded.

CISA published an advisory describing the vulnerabilities found by Krstic in the Osprey Pump Controller on March 23. Ten individual advisories describing each flaw were also published recently on Zero Science Lab's website.

The vulnerabilities include remote code execution, cross-site request forgery (CSRF), authentication bypass, cross-site scripting (XSS), command injection, backdoor access, file disclosure, and session hijacking issues.

Many of these flaws can be exploited without authentication, and Krstic told *SecurityWeek* that dozens of controllers are exposed on the internet, including in the case of the client whose network was assessed by Zero Science Lab.

An attacker could exploit the vulnerabilities to remotely hack a system and take complete control of the device. This can allow them to cause disruption through a DoS attack or perform various types of nefarious activities, depending on what the targeted controller is used for.

"An attacker can access the controller, and change pressure, cause havoc, manipulate VFDs [variable frequency drives] or entirely cut down the water supply, depending where the controller is applied," Krstic explained.

According to CISA, the impacted controller is used worldwide in various industries. The agency has advised ProPump and Controls customers to contact the vendor to obtain information on any patches or mitigations.

However, the Zero Science Lab advisories reveal that CISA has assigned this incident a priority rating of 'baseline – negligible', which indicates that it's "highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence".

It's not uncommon for hackers to target water facilities,

including in the United States. CISA and other agencies warned in 2021 that ransomware had hit SCADA systems at three water facilities in the country. The warning came just months after a hacker was caught apparently trying to poison a Florida city’s water supply.

Related: Hacktivist Attacks Show Ease of Hacking Industrial Control Systems

Related: Water Tank Management System Used Worldwide Has Unpatched Security Hole

Related: Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack

> *Unpatched Security Flaws Expose Water Pump Controllers to Remote Hacker Attacks*