National Cyber Security Centre

2312010119-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Active Exploitation of Unitronics PLCs

Friday 1st December, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

The NCSC is aware that Unitronics Programmable Logic Controllers (PLCs) which are used in some Water and Wastewater Systems are under active exploitation within Ireland.

The devices are used to monitor various stages and processes of water and wastewater treatment, including turning on and off pumps at a pump station to fill tanks and reservoirs, flow pacing chemicals to meet regulations, gathering compliance data for monthly regulation reports, and announcing critical alarms to operations.

Products Affected

- Unitronics PLC devices

Impact

Unauthorised access to these devices may allow an attacker to impact the ability of the Water and Wastewater facilities to provide clean potable water to their local communities.

Recommendations

The NCSC recommends performing the following actions:

- Change default passwords on PLCs ensuring a strong password is utilised.
- Require multifactor authentication for all remote access to the OT network, including from the IT network and external networks.
- Disconnect the PLC from the open internet.
- Back up the logic and configurations on any Unitronics PLCs to enable fast recovery. Become familiar with the process for factory resetting and deploying configurations to a device in the event of being hit by cryptoware.
- If possible, utilize a TCP port that is different than the default port TCP 20256.
- Update PLC/HMI to the latest version provided by Unitronics.

The NCSC recommends that any organisation that is affected by attacks on their Water and Wastewater Systems OT systems provide details of these attacks to the NCSC and contact their local Garda station as soon as possible.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie