ACTIVITY ALERT

AA20-133B NUMBER

May 12, 2020 DATE

Cyber Threat Actor Disrupts Israeli Water Infrastructure

KEY TAKEAWAYS

- Cyber threat actors accessed and modified the control logic on multiple internet-accessible programmable logic controllers (PLCs) at several Israeli water sector facilities.
- The modifications caused the controllers to exhibit unexpected behavior but did not result in the physical destruction of equipment.
- Critical infrastructure owner operators are encouraged to implement recommended mitigations to reduce the likelihood and impact of similar attacks.

EXECUTIVE SUMMARY

On April 23, 2020, the Israeli National Cyber Directorate (INCD) received reports from multiple Israeli water sector owner operators describing abnormal equipment operation. INCD's investigation found the events to be the result of a coordinated cyberattack by an unknown threat actor who accessed internet-exposed programmable logic controllers. Although the attack resulted in unexpected process behavior, it did not result in damage to equipment. In this alert, the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Environmental Protection Agency (EPA), and U.S. Department of Energy (DOE) summarize INCD's findings and recommend mitigations that critical infrastructure owner operators—especially those with internet-exposed control system assets—should consider implementing to protect against similar attacks.

TECHNICAL DETAILS[1]

On April 23, 2020, the INCD received reports from multiple Israeli water sector owner operators describing abnormal equipment operation at their facilities.[2] INCD's investigation found the events to be the result of a coordinated cyberattack by an unknown threat actor who accessed internet-accessible PLCs at several geographically distinct water sector facilities.

Affected equipment included controllers manufactured by multiple vendors. The controllers did not require any authentication and were accessed over standard ports specific to each vendor. Most likely, using vendor engineering software, the threat actor modified the process logic and then uploaded the modified process logic to the controllers. This resulted in unexpected controller behavior and changes to the physical process, which alerted operators. Despite these effects, the attack did not result in damage to equipment or loss of safety.

CISA mapped activities observed in the attack to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for Industrial Control Systems (ICS) framework:

- **Initial Access.** The threat actor connected to *Internet Accessible* PLCs [T883] that required no authentication.
- **Command and Control**. Using *Commonly Used Ports* [T885] and *Standard Application Layer Protocols* [T869], the threat actor communicated with the controllers and downloaded modified control logic. Specific protocols included S7comm (102/TCP), modbus (502/TCP), and GE SRTP (TCP ports 18245 and 18246).
- **Impair Process Control.** Using vendor engineering software and *Program Downloads* [T843], the threat actor *Modified Control Logic* [T833] and *Modified Parameters* [T836] on the PLCs.
- **Impact.** Modification of controller logic resulted in adversary *Manipulation of Control* [T831] and disruption to physical processes.

MITIGATIONS

CISA, EPA, and DOE recommend Water and Wastewater Systems Sector owner operators implement the following mitigations to defend against similar attacks.[3]

Network and Architectural Mitigations

- Use *Network Segmentation* [M1030] to protect PLCs and workstations from direct exposure to the internet. Implement secure network architectures utilizing demilitarized zones (DMZs), firewalls, jump servers, and one-way communication diodes.
- Ensure all communications to remote devices use a secure virtual private network (VPN) with multifactor authentication and strong encryption. Verify that such access represents a legitimate business need.

---

[1] This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework. See the MITRE ATT&CK for Enterprise and ATT&CK for Industrial Control Systems (ICS) frameworks for all referenced threat actor techniques and mitigations.

[2] INCD's Alert: https://www.gov.il/he/departments/publications/reports/scadaalert

[3] EPA's Cybersecurity 101 for Water Utilities: https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P100KL4T.txt

- *Filter Network Traffic* [M1037] using Internet Protocol (IP) whitelisting or geo-blocking where appropriate.
- Connect remote PLCs and workstations to network intrusion detection systems where feasible. Capture and review access logs from these systems.
- Encrypt network traffic when supported by the operational technology (OT) system components to prevent sniffing and man-in-the-middle attacks.

Access Mitigations

- When possible, enable authentication on OT system components.
- Implement secure *Password Policies* [M1027]. Require the use of strong, complex passwords and prohibit the use of default passwords on all devices, including controllers and OT equipment.
- Use *User Account Management* [M1018] to remove, disable, or rename any default system accounts wherever possible.
- Monitor the creation of administrator-level accounts by third-party vendors with robust and *Privileged Account Management* [M1026] policies and procedures.
- Implement *Account Lockout Policies* [M1036] to reduce risk from brute force attacks.

Additional Mitigations

- Implement integrity checks of controller process logic against a known good baseline.
- Where possible, ensure process controllers are prevented from remaining in remote program mode while in operation.
- Lock or limit setpoints in control processes to reduce the consequences of unauthorized controller access.
- Use internet search engines such as Shodan to *Audit* [M1047] and identify internet-accessible OT devices on your network.
- Implement and regularly test *Data Backup* [M1053] processes to support recovery in the event of data loss.

RESOURCES

- INCD's Alert: https://www.gov.il/he/departments/publications/reports/scadaalert
- CISA's Cyber Security Evaluation Tool: https://www.us-cert.gov/ncas/current-activity/2019/11/04/cset-version-92-now-available
- CISA's Tip on Securing Network Infrastructure Devices: https://www.us-cert.gov/ncas/tips/ST18-001
- CISA's Tip on Supplementing Passwords: https://www.us-cert.gov/ncas/tips/ST05-012
- CISA's Tip on Enterprise VPN Security: https://www.us-cert.gov/ncas/alerts/aa20-073a
- EPA's Cybersecurity 101 for Water Utilities: https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P100KL4T.txt
- DOE's Cybersecurity Capability Maturity Model (C2M2): https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

- American Water Works Association (AWWA) Guidance and Assessment Tool: www.awwa.org/cybersecurity
- WaterISAC Cybersecurity Fundamentals: https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

CONTACT INFORMATION

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- CISAServiceDesk@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found at http://www.us-cert.gov/.

Recipients may reach out to EPA at Schmelling.dan@epa.gov or DOE at doeares@hq.doe.gov.

FEEDBACK

CISA strives to make this report a valuable tool for our partners and welcomes feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: https://www.us-cert.gov/forms/feedback.