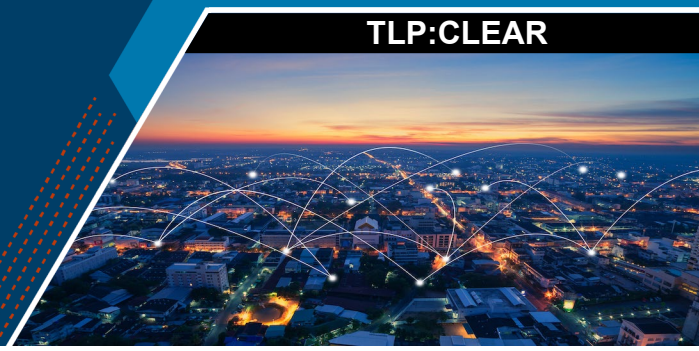
Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity



MS-ISAC® Multi-State Information Sharing & Analysis Center®

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against *insecure and misconfigured* OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

Historically, these hacktivists have been known to exaggerate their capabilities and impacts to targets. Since 2022, they have claimed on social media to have conducted cyber operations (such as distributed denial of service, data leaks, and data wiping) against a variety of North American and international organizations. Based on victim incident reporting, this activity has caused limited disruption to operations.

2024 Year-to-Date Activity

In early 2024, the authoring organizations observed pro-Russia hacktivists targeting vulnerable industrial control systems in North America and Europe. CISA and the FBI have responded to several U.S.-based WWS victims who experienced limited physical disruptions from an unauthorized user remotely manipulating HMIs. Specifically, pro-Russia hacktivists manipulated HMIs, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hacktivists maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the WWS operators. Some victims experienced minor tank overflow events; however, most victims reverted to manual controls in the immediate aftermath and quickly restored operations.

Remote Access to HMIs

The authoring organizations have observed pro-Russia hacktivists using a variety of techniques to gain remote access to HMIs and make changes to the underlying OT. These techniques include:

- Using the VNC Protocol to access HMIs and make changes to the underlying OT. VNC is used for remote access to graphical user interfaces, including HMIs that control OT systems.
- Leveraging the VNC Remote Frame Buffer Protocol to log into HMIs to control OT systems.
- Leveraging VNC over Port 5900 to access HMIs by using default credentials and weak passwords on accounts not protected by multifactor authentication.

Note: Several HMIs compromised by these hacktivists were unsupported legacy, foreign-manufactured devices rebranded as U.S. devices.

MITIGATIONS

The authoring organizations recommend critical infrastructure organizations implement the following mitigations to defend against this activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

Network Defenders

Pro-Russia hacktivists have exploited cybersecurity weaknesses, including poor password security and exposure to the internet. To safeguard against this threat, the authoring organizations urge organizations to:

Harden HMI Remote Access

- **Disconnect all HMIs, such as the touchscreens used to monitor or make changes to the system, or programmable logic controllers (PLCs), from the public-facing internet.** If remote access is necessary, implement a firewall and/or virtual private network (VPN) with a strong password and multifactor authentication to control device access [CPG 2.W] [CPG 2.X].
- **Implement multifactor authentication for all access to the OT network.** For additional information, see CISA's More than a Password [CPG 2.H].

- **Immediately change all default and weak passwords on HMIs and use a strong, unique password.** Ensure the factory default password is not in use. Open the remote settings panel to confirm the old password is no longer shown [CPG 2.A] [CPG 2.B].
- **Keep VNC updated with the latest version available** and ensure all systems and software are up to date with patches and necessary security updates.
- **Establish an allowlist** that permits only authorized device IP addresses. The allowlist can be refined to specific times of the day to further obstruct malicious threat actor activity; organizations are encouraged to establish alerting for monitoring access attempts.
  - **Note:** An allowlist is not a complete security solution by itself but may increase the level of effort necessary for a threat actor to compromise a device.
- **Log remote logins to HMIs,** taking note of any failed attempts and unusual times [CPG 2.T].

Strengthen Security Posture

- **Integrate cybersecurity considerations into the conception, design, development, and operation of OT systems.** For additional information, see the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER)'s publication on Cyber-Informed Engineering.
- **Practice and maintain the ability to operate systems manually** [CPG 5.A].
- **Create backups** of the engineering logic, configurations, and firmware of HMIs to enable fast recovery. Familiarize your organization with factory resets and backup deployment [CPG 2.R].
- **Check the integrity of PLC ladder logic or other PLC programming languages** and diagrams and check for any unauthorized modifications to ensure correct operation. Adversaries may try to maintain persistence or stealthily operate the device in an unsafe way by changing the configurations and ladder logic.
- **Update and safeguard network diagrams** to reflect both the IT and OT networks [CPG 2.P]. Operators should apply the principles of least privilege and need to know for individuals' access to network diagrams. Maintain awareness of internal and external solicitation efforts (both malicious and benign) to obtain network architectures and restrict mapping to trusted personnel. Consider using encryption, authentication, and authorization techniques to secure network diagram files and implement access control and audit logs to monitor and restrict who can view or modify your network diagrams.
- **Be aware of cyber/physical-enabled threats.** Adversaries may attempt to obtain network credentials by various physical means, including official visits, tradeshow and conference conversations, and through social media platforms.
- **Take inventory and determine the end-of-life status of all HMIs** [CPG 1.A]. Replace end-of-life HMIs as soon as feasible.
- **Implement software and hardware limits** to the manipulation of physical processes, limiting the impact of a successful compromise. This can be completed through using operational interlocks, cyber-physical safety systems, and cyber-informed engineering.

Limit Adversarial Use of Common Vulnerabilities

- **Reduce risk exposure.** U.S. organizations can utilize a range of CISA services at no cost, including scanning and testing, to help organizations reduce exposure to threats by mitigating attack vectors. CISA Cyber Hygiene services can help provide additional review of internet-accessible assets and provide regular reports on steps to take to mitigate vulnerabilities. Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services," to get started. UK organizations can use NCSC's free Early Warning service.
- **Assess your security posture.** CISA's regional Cybersecurity Advisors provide CPG assessments to help organizations understand their current security posture. Reach out to your regional CISA office to schedule an assessment.

OT Device Manufacturers

Although critical infrastructure organizations can take steps to mitigate risks, it is ultimately the responsibility of the OT device manufacturer to build products that are secure by design and default. The authoring organizations urge device manufacturers to take ownership of the security outcomes of their customers in line with the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software and CISA's Secure by Design webpage.

- **Eliminate default and require strong passwords.** The use of default credentials is a top weakness that threat actors exploit to gain access to systems. Manufacturers can eliminate this problem at scale through any of the approaches recommended in CISA's Secure by Design Alert on this topic.
- **Mandate multifactor authentication for privileged users.** Changes to engineering logic or configurations are safety-impacting events in critical infrastructure. Any changes should require multifactor authentication.
- **Include logging at no additional charge.** Change and access control logs allow operators to track safety-impacting events in their critical infrastructure. These logs should be free and use open standard logging formats.
- **Publish Software Bills of Materials (SBOM).** Vulnerabilities in underlying software libraries can affect wide swathes of devices. Without an SBOM, it is nearly impossible for a critical infrastructure system owner to measure and mitigate the impact a vulnerability has on their existing systems.

Additionally, see CISA's Secure by Design Alert on how software manufacturers can shield web management interfaces from malicious cyber activity. By using secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing tiered security software and logs, monitoring, and making routine updates.

RESOURCES

Entities requiring additional support for implementing any of the mitigations in this advisory should contact their regional CISA Cybersecurity Advisor and/or EPA for assistance. Five key resources organizations should reference include:

- NSA, CISA: Recommended Immediate Actions to Reduce Exposure Across all OT and Control Systems
- CISA, EPA: Water and Wastewater Systems Sector Toolkit
- CISA, EPA, FBI: Top Cyber Actions for Securing Water Systems
- Food and Agriculture Information Sharing & Analysis Center (Food and Ag-ISAC): Cybersecurity Guide for Small and Medium Enterprises
- DOE, National Association of Regulatory Utility Commissioners (NARUC): Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources

Additional resources include:

- NCSC-UK: Operational Technology Guidance
- EPA: Cybersecurity for the Water Sector
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: More than a Password
- DOE: Cyber-Informed Engineering
- CISA: Cyber Hygiene Services
- CISA: Shifting the Balance of Cybersecurity Risk - Principles and Approaches for Secure by Design Software
- CISA: Secure by Design
- CISA: Secure by Design Alert - How Manufacturers Can Protect Customers by Eliminating Default Passwords
- CISA: Secure by Design Alert - How Software Manufacturers Can Shield Web Management Interfaces from Malicious Cyber Activity

REPORTING

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this fact sheet to:

- CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- Water and Wastewater Systems Sector organizations should contact the EPA Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness.
- State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).
- The Water Information Sharing & Analysis Center (WaterISAC) encourages members to share information by emailing analyst@waterisac.org, calling 866-H2O-ISAC, or using the online incident reporting form.
- Entities required to report incidents to DOE-CESER should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov. DOE also encourages energy entities to report information to their relevant energy ISACs:
  - Downstream Natural Gas (DNG-ISAC): analyst@dngisac.com
  - Electricity (E-ISAC): operations@eisac.com
  - Oil & Natural Gas (ONG-ISAC): soc@ongisac.org

International organizations:

- UK organizations are encouraged to report any suspected compromises to the NCSC via their incident reporting website.
- Canadian organizations should report incidents by emailing CCCS at contact@cyber.gc.ca.

ACKNOWLEDGEMENTS

The DNG-ISAC and WaterISAC contributed to this fact sheet.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.

VERSION HISTORY

May 1, 2024: Initial version.