IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA

Published: 2024-12-18 · Archived: 2026-04-05 20:15:02 UTC

1. Address operational technology connected insecurely to the internet.
2. Implement multifactor authentication.
3. Use strong, unique passwords.
4. Check PLCs for default or no passwords.

Summary

Note: This updated joint Cybersecurity Advisory reflects new investigative and analytic insights for network defenders on malicious cyber activities conducted by advanced persistent threat (APT) cyber actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC). This advisory includes recent and historically observed tactics, techniques, and procedures (TTPs) to help organizations protect their critical infrastructure systems against such activities.

Originally published Dec. 1, 2023, updates to this advisory include:

- **Dec. 18, 2024**
  - New information on the extent of the activity, including newly observed TTPs employed by IRGC-affiliated APT cyber actors targeting U.S. and global critical infrastructure.
  - Mapping of these newly observed TTPs to additional MITRE ATT&CK® Tactics and Techniques.
  - New recommended mitigations that organizations should take to protect their infrastructure, based on the new TTPs.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Environmental Protection Agency (EPA), the Israel National Cyber Directorate (INCD), the Canadian Centre for Cyber Security (CCCS), and the United Kingdom's National Cyber Security Centre (NCSC)—hereafter referred to as "the authoring agencies"—are releasing this updated joint advisory to warn network defenders of continued malicious cyber activity by IRGC-affiliated APT cyber actors. This joint advisory provides TTPs obtained from extensive FBI investigation on this activity.

Background Information

The Iranian Government charged the IRGC, an armed force, with defending Iran's revolutionary regime from perceived internal and external threats. The IRGC is designated as a foreign terrorist organization by the United States and Canada. In November 2023, IRGC-affiliated cyber actors using the persona "CyberAv3ngers" began actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs)

and human machine interfaces (HMIs). The IRGC-affiliated cyber actors left a defacement image stating, “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target.” The victims spanned multiple U.S. states and foreign countries. These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and used in other industries including, but not limited to, energy, food and beverage manufacturing, transportation systems, and healthcare. The PLCs may be rebranded and appear as originating from different manufacturers and companies.

Complementing a previously published CISA Alert, the authoring agencies are releasing this updated joint advisory to share TTPs associated with IRGC cyber operations. The authoring agencies urge all organizations, especially those within critical infrastructure sectors, to apply the recommendations listed in the **Mitigations** section of this advisory to reduce the risk of compromise from these IRGC-affiliated cyber actors.

Overview of Updated Information

This advisory provides observed TTPs the authoring agencies assess are likely associated with this IRGC-affiliated APT. The late 2023 campaign conducted by CyberAv3ngers compromised additional Unitronics version types, including older PLC models, than were previously outlined. The IRGC-affiliated APT cyber actors also developed custom ladder logic files to download for each of these device types. Previously unreported TTPs also outline how the actors supplanted existing ladder logic files with their own, renamed devices likely to forestall owner access, reset software versions to older versions, disabled upload and download functions, and changed the default port numbers. With this type of access, deeper device and network level accesses are available and could render additional, more profound cyber-physical effects on processes and equipment. Additionally, the NCSC observed the targeting of PLC devices, including in the United Kingdom, likely as part of a wider cyber campaign against Israel and Israeli-made technology. This targeting of PLCs poses an ongoing risk to UK organizations that utilize these components in their operational technology (OT) systems. For more information on Iranian state-sponsored malicious cyber activity, see CISA’s Iran Cyber Threat Overview and Advisories webpage and the FBI’s Iran Threat webpage.

Download the PDF version of this report:

For a downloadable copy of the indicators of compromise (IOCs), see:

Note: These IOCs are from the original joint advisory published Dec. 1, 2023, and are not current.

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 16. See **Table 1** through **Table 4** for threat actor activity mapped to MITRE ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK’s Best Practices for MITRE ATT&CK Mapping and CISA’s Decider Tool.

Overview and History of Threat Actor Activity

CyberAv3ngers is an Iranian IRGC-affiliated cyber persona (also known as CyberAveng3rs or Cyber Avengers) that has claimed responsibility for numerous attacks against critical infrastructure organizations primarily in the

water and energy sectors in the United States, Israel, and other countries.[1][2][3][4][5][6][7][8][9][10] Since 2020, CyberAv3ngers has claimed responsibility for cyberattacks in Israel, although several of these claimed compromises of critical infrastructure organizations in Israel are false.[3] In October 2023, CyberAv3ngers claimed credit on their Telegram Channel for cyberattacks against Israel-based PLCs. The PLCs were internet-facing, used Unitronics' default passwords or no password, and connected to default ports—vulnerabilities that were likely exploited by the actors. CyberAv3ngers also reportedly has connections to another IRGC-linked group known as Soldiers of Solomon. The observed activity includes the following:

- Between Sept. 13, 2023, and Oct. 30, 2023, the CyberAv3ngers Telegram channel displayed both legitimate and false claims of multiple cyberattacks against Israel. CyberAv3ngers targeted Israeli PLCs in the water, energy, shipping, and distribution sectors.
- Beginning on Nov. 22, 2023, IRGC cyber actors accessed multiple U.S.-based WWS facilities that operate HMI-capable Unitronics Vision Series PLCs likely by compromising internet accessible devices with default or no passwords. The targeted PLCs displayed the defacement message, "You have been hacked, down with Israel. Every equipment 'made in Israel' is Cyberav3ngers legal target."

(Update Dec. 18, 2024)

Threat Actor Activity Against U.S.-Based Unitronics Devices

Between November 2023 and January 2024, CyberAv3ngers targeted U.S.-based Unitronics PLC devices used in multiple critical infrastructure industries, including the WWS Sector, likely in four separate waves of cyberattacks. The actors compromised at least 75 devices, including at least 34 in the WWS Sector in the United States.

The actors compromised multiple Unitronics Vision Series devices by authenticating to internet-connected devices with communications set to the default TCP port `20256` [T1110]. These devices either had a default password in place or no password [T1078.001]. The actors made multiple changes to the devices to disrupt their functions and prevent remote operators from connecting to the devices to remediate the problem. Actions taken by the actors included the following:

- The actors erased the original ladder logic file on the device and downloaded their own [T1565.001]. Their ladder logic file contained no inputs or outputs. Since the programmed ladder logic is responsible for directing the functioning of the device, the replacement ladder logic file prevented the compromised devices from operating as intended.
- The actors renamed the compromised devices, which delayed the device operators from accessing the devices remotely as the device name was a required field for facilitating remote connections [T1531].
- The actors set the software version of their ladder logic file to an older version [T1565.001]. Resetting the software version prevented the device operators from communicating with the PLC using their engineering workstation. This could only be resolved if the engineering workstation's software version changed to match the software version of the new ladder logic file or if the PLC device was factory reset so the ladder logic would be the latest software version.
- The actors disabled the upload and download functions of the PLC device to prevent the device operators from taking down the splash page [T1499]. Additionally, the actors enabled password protection for the upload settings, preventing device operators from changing the programming remotely [T1531].

- The actors changed the default port number for communicating remotely with the PLC device (from `20256` to `20257`) [T1499].
- The actors did not burn their ladder logic file to the device, preventing the retrieval of the ladder logic file from the device.
- The actors uploaded a splash page with the aforementioned defacement message to the HMI screen, which prevented operators from reading anything the display screen would normally show, such as input and output readings [T1491.001]. In at least one instance the actors displayed a text file with the same message on an older device that could not display a graphic image.

Multiple versions of the Unitronics devices were compromised, including older models. The actors developed custom ladder logic files to download for each device type.

With this type of access, and depending on the device's configuration, deeper device and network level accesses are available and could render additional, more profound cyber-physical effects on processes and equipment. Organizations should consider and evaluate their systems for these possibilities.

(Update End)

Indicators of Compromise

Update Dec. 18, 2024:

The indicators provided in this advisory's initial publication have been removed as they are outdated. For historic reference, see AA23-335A IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (Original Version).

(Update End)

MITRE ATT&CK Tactics and Techniques

See **Table 1 through Table 4** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool .

Table 1: Credential Access

Technique Title	ID	Use
Brute Force	T1110	The actors used brute force to gain access to Valid Accounts.

Table 2: Lateral Movement

Technique Title	ID	Use
Valid Accounts: Default Accounts	T1078.001	The actors compromised multiple devices via default credentials.

Table 3: Impact Techniques

Technique Title	ID	Use
Stored Data Manipulation	T1565.001	The actors erased the original ladder logic file on compromised devices. The actors set the software version of their ladder logic file to an older version, which prevented device operators from communicating with the PLC using their engineering workstation. This could only be resolved when the engineering workstation's software version changed to match the software version of the new ladder logic file or if the PLC device was factory reset so the ladder logic would be the latest software version.
Account Access Removal	T1531	The actors renamed the compromised devices so that device operators could no longer access them. The actors enabled password protections for the upload functions to prevent device operators from changing the programming remotely.
Endpoint Denial of Service	T1499	The actors disabled the upload and download functions of the PLC device to prevent the device operators from taking down the splash page.
Defacement: Internal Defacement	T1491.001	The actors uploaded a splash page to the HMI screen to display a message regarding the hacking.

Table 4: Command and Control

Technique Title	ID	Use
Endpoint Denial of Service	T1499	The actors changed the default port number for communicating remotely with the PLC device.

Mitigations

The authoring agencies recommend critical infrastructure organizations, including WWS Sector facilities, implement the following mitigation and detection strategies to improve organizational cybersecurity posture to defend against IRGC-affiliated 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.

Note: The mitigations below are based on threat actor activity against Unitronics PLCs, but threat actors have targeted multiple internet-exposed PLCs in 2024.[1] These mitigations should be applied to any internet-facing PLCs.

Network Defenders

(Updated Dec. 18, 2024)

The cyber threat actors accessed the affected devices—Unitronics Vision Series PLCs—by authenticating to internet-connected devices using default or no passwords. To safeguard against this threat, the authoring agencies urge organizations to consider the following:

Immediate steps to prevent the attack:

- (Updated Dec. 18, 2024) **Upgrade engineering workstations to 9.9.00 VisiLogic software and upgrade the firmware of all Vision series PLC/HMI devices** to the newest firmware for that model, [CPG 2.A], ensuring a strong password is used.
    - For more information, see Unitronics' blog Unitronics Cybersecurity for Vision and Samba PLC Series and Release notes for VisiLogic 9.9.00.
- **Replace all default passwords on PLCs and HMIs with a strong password.** [CPG 2.A] In particular, ensure the Unitronics PLC default password is not in use. Apply new security-related ladder logic elements to the project files on these devices, to include TCP/IP passwords, upload project files passwords, INFO mode passwords, and SD card passwords.
- **Disconnect the PLC from the public-facing internet** [CPG 2.X]. Either disable the capability for remotely programming PLCs or require a strong password for remotely programming the PLC. Also change the default port, default PLC device name, and place behind a firewall that can detect attempted remote brute-forcing for the device password.

(Update End)

Follow-up steps to strengthen security posture:

- **Implement multifactor authentication** [CPG 2.H] for access to the OT network whenever applicable.
- If remote access is required, **implement a network proxy, gateway, firewall and/or virtual private network (VPN) in front of the PLC to control network access**.
    - A VPN or gateway device can enable multifactor authentication for remote access even if the PLC does not support multifactor authentication. Implement security rules on these higher-level network security mechanisms that prevent the type of repeated and sustained login attempts that would be seen during a brute force attack. When possible, implement a device control list for workstations sending messages or connecting to OT components.
- **Keep Unitronics and other PLC devices updated with the latest software patches by the manufacturer**.
- **Confirm third-party vendors apply the above recommended countermeasures** to mitigate exposure of these devices and all installed equipment.

(Updated Dec. 18, 2024)

- **Implement network segmentation** [CPG 2.F] through the use of network proxies, gateways, and firewalls and/or through the use of the Purdue Model to establish multiple levels and zones.
- **Adopt mature asset management processes** and understand which assets are being exposed, why they are being exposed, and their support and patch status.
- **Periodically inventory internet accessible devices** [CPG 1.A] to identify any unexpected devices connected to the network.
- **Configure external and internal firewalls to block traffic using common ports associated with network protocols that are unnecessary for the particular network segment.**
- **Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs**.
    - Centralized authentication techniques can help manage the large number of field controller accounts needed across the industrial control system (ICS).
- **Disable any unused authentication methods, logic, or features,** such as default authentication keys.
- **Use a role-based mechanism to limit operating mode changes to required authenticated users only.**
    - Physical mechanisms (e.g., keys) can also be used to prevent unauthorized operating mode changes.
- **Implement device management systems** that can authenticate all network messages to prevent unauthorized system changes.
- **Ensure all field controllers require users to authenticate for all management sessions.**
- **Use host-based allowlists to prevent devices from accepting connections from unauthorized systems and ensure they can only connect with known workstations.**
- **Implement network intrusion detection and prevention systems** whenever possible to identify malicious activity.
    - Use this to monitor for logon activity for unexpected or unusual access to devices from the internet. [11]
- **Retain cold-standby or replacement hardware of similar models** to ensure continued operations of critical functions if the primary system is compromised or unavailable [CPG 2.R].[12]
    - Create and test strong backups of the logic and configurations of PLCs to enable fast recovery.
- **Utilize watchdog timers,** when possible, to enable quick detection of unresponsive systems.
- **Monitor asset management systems for device configuration changes,** which can be used to understand expected parameter settings.
- **Monitor the content of network traffic for the following**:
    - Unusual logins to internet-connected devices or unexpected protocols to/from the internet.
    - Functions of ICS management protocols that change an asset's operating mode or modify programs.
    - Unexpected protocols connected to ports that are mismatched with the protocols that would normally connect to these ports.[11] Block all non-used high ephemeral ports and monitor for attempted connections using standard protocols on non-standard ports [CPG 2.V].

(Update End)

In addition, the authoring agencies recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, as well as reduce the impact and

risk of compromise by cyber threat actors:

- **Reduce risk exposure.** CISA offers a range of services at no cost, including scanning and testing, to help organizations reduce exposure to threats via mitigating attack vectors. CISA Cyber Hygiene services can help provide additional review of organizations' internet accessible assets. Email vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.
- **(Updated Dec. 18, 2024)** U.K. organizations can sign up for the free NCSC Early Warning service to receive email alerts tailored to the cyber threat for your organization's IP address. **(End Update)**

Device Manufacturers

Although critical infrastructure organizations using Unitronics (including rebranded Unitronics) PLC devices can take steps to mitigate the risks, it is ultimately the responsibility of the device manufacturer to build products that are secure by design and default. The authoring agencies urge device manufacturers to take ownership of their customers' security outcomes by following the principles in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, primarily:

- Do not ship products with default passwords; instead, either ship products with random initial passwords or require users to change the password upon first use.
- **(Updated Dec. 18, 2024)** Change the manufacturers' default settings to prevent exposing administrative interfaces to the internet. **(End Update)**
- Do not charge additional fees for basic security features needed to operate the product securely.
- Support multifactor authentication, including via phishing-resistant methods.

By using secure by design tactics, software manufacturers can make 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.

For more information on common misconfigurations and guidance on reducing their prevalence, see joint advisory NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing any existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 1** through **Table 4**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.

5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

- EPA: Cybersecurity for the Water Sector
- CISA: Water and Wastewater Systems Sector
- CISA Alert: Exploitation of Unitronics PLCs used in Water and Wastewater Systems
- CISA: Iran Cyber Threat Overview and Advisories
- FBI: The Iran Threat
- CISA, MITRE: Best Practices for MITRE ATT&CK Mapping
- CISA: Decider Tool
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: Cyber Hygiene Services
- CISA: Shifting the Balance of Cybersecurity Risk - Principles and Approaches for Secure by Design Software
- CISA: Secure by Design Alert - How Software Manufacturers Can Shield Web Management Interfaces from Malicious Cyber Activity
- CISA, NSA: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
- CISA: Secure by Design and Default
- CCCS: Cyber Security Readiness Goals: Securing Our Most Critical Systems

References

1. Dark Reading: Pro-Iranian Attackers Claim to Target Israeli Railroad Network
2. Industrial Cyber: Digital Battlegrounds - Evolving Hybrid Kinetic Warfare
3. Bleeping Computer: Israel’s Largest Oil Refinery Website Offline After DDoS Attack
4. Dark Reading: Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers
5. X: @CyberAveng3rs
6. MITRE: CyberAv3ngers
7. VeroNews: Hackers in Iran Attack Computer at Vero Utilities, December 15, 2023
8. CBS News: Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group
9. Dragos: The Rising Tide of Water Utility Cyber Threats: How Dragos Shield Water Systems
10. Claroty: From Exploits to Forensics: Unraveling the Unitronics Attack
11. Gardiner, J., Cova, M., and Nagaraja, S.: Command & Control Understanding, Denying and Detecting
12. M. Rentschler and H. Heine. The Parallel Redundancy Protocol for Industrial IP Networks

Incident Reporting Contact Information

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

- CISA via CISA's 24/7 Operations Center (Contact@mail.cisa.dhs.gov or 884-729-2472) 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.
- State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

Canadian organizations are encouraged to report incidents by emailing CCCS at contact@cyber.gc.ca.

U.K. organizations are encouraged to report incidents to https://report.ncsc.gov.uk/ (monitored 24 hours).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies 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 CISA and co-sealers.

Version History

December 2024: Updates noted throughout.
Dec. 14, 2023: Added CVE, patch information, and IOC descriptions.
Dec. 1, 2023: Initial version.
