JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-336A

December 2, 2023

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

SUMMARY

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD)—hereafter referred to as "the authoring agencies"—are disseminating this joint Cybersecurity Advisory (CSA) to highlight continued malicious cyber activity against operational technology devices by Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated Advanced Persistent Threat (APT) cyber actors.

Actions to take today to mitigate malicious activity:

- Implement multifactor authentication.
- Use strong, unique passwords.
- Check PLCs for default passwords.

The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona “CyberAv3ngers” are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies. In addition to the recent CISA Alert, the authoring agencies are releasing this joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with IRGC cyber operations.

Since at least November 22, 2023, these IRGC-affiliated cyber actors have continued to compromise default credentials in Unitronics devices. 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 span multiple U.S. states. The authoring agencies urge all organizations,

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA’s 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. 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 client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

especially critical infrastructure organizations, to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from these IRGC-affiliated cyber actors.

This advisory provides observed IOCs and TTPs the authoring agencies assess are likely associated with this IRGC-affiliated APT. For a downloadable copy of IOCs, see AA23-335A.stix. 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.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See Table 1 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

CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers) is an Iranian IRGC cyber persona that has claimed responsibility for numerous attacks against critical infrastructure organizations.[1],[2],[3],[4],[5],[6] The group claimed responsibility for cyberattacks in Israel beginning in 2020. CyberAv3ngers has falsely claimed they compromised several critical infrastructure organizations in Israel.[3] CyberAv3ngers also reportedly has connections to another IRGC-linked group known as Soldiers of Solomon.

Most recently, CyberAv3ngers began targeting U.S.-based WWS facilities that operate Unitronics PLCs.[1] The threat actors compromised Unitronics Vision Series PLCs with human machine interfaces (HMI). These compromised devices were publicly exposed to the internet with default passwords and by default are on TCP port 20256.

These PLC and related controllers are often exposed to outside internet connectivity due to the remote nature of their control and monitoring functionalities. The compromise is centered around defacing the controller's user interface and may render the PLC inoperative. 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. It is not known if additional cyber activities deeper into these PLCs or related control networks and components were intended or achieved. Organizations should consider and evaluate their systems for these possibilities.

Threat Actor Activity

The authoring agencies have observed the IRGC-affiliated activity since at least October 2023, when the actors claimed credit for the cyberattacks against Israeli PLCs on their Telegram channel. Since November 2023, the authoring agencies have observed the IRGC-affiliated actors target multiple U.S.-based WWS facilities that operate Unitronics Vision Series PLCs. Cyber threat actors likely compromised these PLCs since the PLCs were internet-facing and used Unitronics' default password. Observed activity includes the following:

- Between September 13 and October 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.
- On October 18, 2023, the CyberAv3ngers-linked Soldiers of Solomon claimed responsibility for compromising over 50 servers, security cameras, and smart city management systems in Israel; however, majority of these claims were proven false. The group claimed to use a ransomware named “Crucio” against servers where the webcams camera software operated on port 7001.
- Beginning on November 22, 2023, IRGC cyber actors accessed multiple U.S.-based WWS facilities that operate Unitronics Vision Series PLCs with an HMI likely by compromising internet-accessible devices with default passwords. The targeted PLCs displayed the defacement message, “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is Cyberav3ngers legal target.”

INDICATORS OF COMPROMISE

See Table 1 for observed IOCs related to CyberAv3nger operations.

Table 1: CyberAv3nger IOCs

Indicator	Type	Fidelity	Description
BA284A4B508A7ABD8070A427386E93E0	MD5	Suspected	MD5 hash associated with Crucio Ransomware
66AE21571FAEE1E258549078144325DC9DD60303	SHA1	Suspected	SHA1 hash associated with Crucio Ransomware
440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3	SHA256	Suspected	SHA256 hash associated with Crucio Ransomware
178.162.227[.]180	IP address		
185.162.235[.]206	IP address		

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 2 for referenced threat actor tactics and techniques in this advisory.

Table 2: Initial Access

Technique Title	ID	Use
Brute Force Techniques	T1110	Threat actors obtained login credentials, which they used to successfully log into Unitronics devices and provide root-level access.

MITIGATIONS

The authoring agencies recommend critical infrastructure organizations, including WWS sector facilities, implement the following mitigations to improve your organization's cybersecurity posture to defend against CyberAv3ngers 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 below mitigations are based on threat actor activity against Unitronics PLCs but apply to all internet-facing PLCs.

Network Defenders

The cyber threat actors likely accessed the affected devices—Unitronics Vision Series PLCs with HMI—by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet. To safeguard against this threat, the authoring agencies urge organizations to consider the following:

Immediate steps to prevent the attack:

- Change all default passwords on PLCs and HMIs and use a strong password. Ensure the Unitronics PLC default password is not in use.
- Disconnect the PLC from the public-facing internet.

Follow-on steps to strengthen your security posture:

- Implement multifactor authentication for access to the operational technology (OT) network whenever applicable.
- If you require remote access, implement a 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.
- Create strong backups of the logic and configurations of PLCs to enable fast recovery. Familiarize yourself with factory resets and backup deployment as preparation in the event of ransomware activity.
- Keep your Unitronics and other PLC devices updated with the latest versions by the manufacturer.
- Confirm third-party vendors are applying the above recommended countermeasures to mitigate exposure of these devices and all installed equipment.

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

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 the security outcomes of their customers 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.
- Do not expose administrative interfaces to the internet by default, and take steps to introduce friction should a device be placed in an insecure state.
- Do not charge extra 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 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.

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 and Default 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 your 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 2).
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 - Web Page
- 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

REPORTING

All organizations should report suspicious or criminal activity related to information in this CSA to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or IC3.gov. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

Additionally, the WaterISAC encourages members to share information by emailing analyst@waterisac.org, calling 866-H2O-ISAC, or using the online incident reporting form. State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

REFERENCES

[1] CBS News: Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group
[2] Dark Reading: Pro-Iranian Attackers Claim to Target Israeli Railroad Network
[3] Industrial Cyber: Digital Battlegrounds - Evolving Hybrid Kinetic Warfare
[4] Bleeping Computer: Israel's Largest Oil Refinery Website Offline After DDoS Attack
[5] Dark Reading: Website of Israeli Oil Refinery Taken Offline by Pro-Iranian Attackers
[6] X: @CyberAveng3rs

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 the authoring agencies.

VERSION HISTORY

December 1, 2023: Initial version.