aria CYBERSECURITY

AZT

Logix®* PLC Attack Protection Recommendation:

The Attack Iranian backed-cyberattack exploits OT systems with Rockwell Programmable Logic Controllers - **CISA Advisory April 7 2026**

Defense Solution: Lockdown OT systems to prevent the attack from doing harm
AZT PROTECT™ Blocks software deployed to activate attack command and control

Situation: CISA and the FBI have highlighted active targeting of industrial environments using Rockwell Automation/Allen-Bradley products and are directly exposed to the internet. The Iranian attack is a sophisticated attack impacting PLCs as well as OT endpoints.

Leveraging CISA CPGs2.0: The following Rapid prevention techniques are recommended below:

Rapid Prevention Steps:

1. **For Rockwell Automation devices, Rockwell recommends placing the physical mode switch on the controller into run position.**
2. **Deploy Rockwell approved ARIA AZT on the Windows OT endpoints** to block the Dropbear SSH application brought in via the attackers from being activated. Thereby stopping the attacker's ability to control and progress the attack to do harm.
3. **Block the PLCs from communicating to the Internet - if possible**. Ideally block all traffic in and out of the PLC subnet, unless this blocks the customers access to control and update the PLCs. Otherwise attempt to limit which IP addresses and protocols can communicate to the PLCs. Details on how to do this: [SD1771 | Security Advisory | Rockwell Automation | US]

More detail on the required steps:

Rockwell Automation : Recommended physical configuration change to the Logix PLCs: Placing the physical mode switch on the controller into run position. Please Refer to: [SD1771 | Security Advisory | Rockwell Automation | US]

ARIA AZT PROTECT™ Can be deployed on OT Windows as well as Linux endpoints to lock them down – blocking the attacker's ability to drop in new software or other executables, as well as block the exploit of those systems OS and applications vulnerabilities. Deployment takes a few hours per site.

Background on how ARIA AZT PROTECT works:

- Connects in as a Windows or Linux OS kernel level driver at Ring Zero
- Sees what is coming down the memory stack as it's about to execute
- Stops unauthorized applications activation as well as updates before they can execute
- Blocks application code-level vulnerability exploits
- AI driven fully automated form of protection.

- Never needs security updates, and can run forever network disconnected
- Removes need for OS security patch updates
  - Ideal for out of support OS based devices/applications.
- Stops the endless need for system reboots for security patching
  - Maximizes uptime impact, reduces risk, while ensuring compliance
- Complies with CISA CPG 2.0 , NIST and ISA standards and security practices

Contact your Rockwell distributor to access ARIA AZT PROTECT & our team of experts

Effective Cybersecurity Starts with a Trusted Partner

For more than 50 years, ARIA Cybersecurity has delivered peace of mind to some of the world's most critical organizations—including the U.S. Department of Defense, mission critical device manufacturers, and large cell tower operators. Our proven solutions and expert team are here to help you protect what matters most.

To learn more about AZT PROTECT, contact us at info@ariacybersecurity.com or visit ariacybersecurity.com/aria-azt-protect/

ARIA Cybersecurity
175 Cabot Street, Suite 210 Lowell, MA 01854. +1 800.325.3110

For more information see:

https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

From Rockwell: [SD1771 | Security Advisory | Rockwell Automation | US]

*Logix® is a registered trademark of Rockwell Automation