Dragos Enabled Defense Against APT Exploits for Rockwell Automation ControlLogix

dragos.com/blog/mitigating-cves-impacting-rockwell-automation-controllogix-firmware/

July 12, 2023

The Dragos Blog

07.12.23 | 4 min read

Dragos, Inc.

Threats

In coordination with the U.S. government, Rockwell Automation has analyzed a novel exploit capability attributed to Advanced Persistent Threat (APT) actors affecting select communication modules by Rockwell Automation in specific ControlLogix EtherNet/IP (ENIP) communication module models, 1756-EN2, 1756-EN3 (CVE-2023-3595), and 1756-EN4 (CVE-2023-3596). The identified vulnerabilities allow for remote code execution with persistence and denial of service (DoS) attacks on the corresponding devices.

As a trusted ICS/OT threat intelligence partner, Dragos worked in advance of the disclosure of CVE-2023-3595 and CVE-2023-3596 to coordinate and help assess the extent of the threat. Dragos leveraged Neighborhood Keeper, its collective defense and anonymized community-wide visibility solution, as well as OT Watch to evaluate and determine the prevalence of vulnerable devices. This enabled Dragos to use real time insights to enhance the detections in partnership with Rockwell Automation. These detections were made immediately available to Dragos Platform customers enrolled into OT Watch and Neighborhood Keeper. In addition, they will be available in the upcoming Knowledge Pack release.

Update: Knowledge Pack KP-2023-004 is now available for all Dragos Platform customers.

The results and impact of exploiting these vulnerabilities vary depending on the ControlLogix system configuration, but they could lead to denial or loss of control, denial or loss of view, theft of operational data, or manipulation of control for disruptive or destructive consequences on the industrial process for which the ControlLogix system is responsible. **Dragos advises all ICS/OT asset owners to identify assets with impacted communications modules and update their Rockwell Automation ControlLogix firmware to the latest version as soon as possible.**

ICS/OT Impact of CVE-2023-3595 & CVE-2023-3596

The affected communications modules are part of the ControlLogix system and are present in multiple industrial verticals, including but not limited to manufacturing, electric, oil and gas, and liquified natural gas. These vulnerabilities affect Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication module series: 1756 EN2*, 1756 EN3*, and 1756 EN4*. Both CVE-2023-3595 and CVE-2023-3596 exist inside the devices' Common Industrial Protocol (CIP) implementation and allow remote code execution with persistence on the EN2* and EN3* modules, and denial of service (DoS) attacks on the EN4* modules respectively.

- CVE-2023-3595 allows for arbitrary manipulation of firmware memory, which could lead to denial or loss of control, denial or loss of view, theft of operational information, or manipulation of control and manipulation of view for disruptive or destructive consequences.

- CVE-2023-3596 could lead to denial or loss of view, or denial of control of the industrial process.

Additional ICS/OT impacts would be dependent on the configuration of the ControlLogix system and how the operation of the process is set up.

Knowing about an APT-owned vulnerability before exploitation is a rare opportunity for proactive defense for critical industrial sectors. The type of access provided by CVE-2023-3595 is similar to the zero-day employed by XENOTIME in the TRISIS attack. Both allow for arbitrary firmware memory manipulation, though CVE-2023-3595 targets a communication module responsible for handling network commands. However, their impact is the same.

Additionally, in both cases, there exists the potential to corrupt the information used for incident response and recovery. The attacker could potentially overwrite any part of the system to hide themselves and stay persistent, or the interfaces used to collect incident response or forensics information could be intercepted by malware to avoid detection. Exploitation of this type of vulnerability renders the communication module untrustworthy, and it would need to be de-commissioned and sent back to the vendor for analysis.

Exploitation in the Wild

An unreleased exploit capability leveraging these vulnerabilities is associated with an unnamed APT (Advanced Persistent Threat) group. Based on analysis by the Dragos Threat Intelligence team using first-party data, as of mid-July 2023 there was no evidence of exploitation in the wild and the targeted victim organizations and industry verticals were unknown. Threat activity is subject to change and customers using affected products could face serious risk if exposed.

Dragos Recommendations for CVE-2023-3595 & CVE-2023-3596

Rockwell Automation has provided patches for all affected products, including hardware series that were out of support. Detection rules have also been provided. Dragos advises that you reference Rockwell Automation’s mitigation and detection guidance, along with our own recommendations, as follows:

- Upgrade firmware to the latest release. 1756-EN2* and EN3* models will need to be upgraded to at least version 11.004 or 5.029, depending on the series. 1756-EN4* models will need to be upgraded to firmware version 5.002. You can find the latest firmware updates here.
- Restrict access to TCP/44818 and UDP/2222 on affected devices. Where applicable or possible, segment these networks away from the internet and other unnecessary networks.

- If possible and not in use by your configuration, disable the CIP Socket Object. Instructions are available here on page 17. To disable, use Logix Designer to send a generic CIP message to set the DisableSocketObj (Attribute 9) on the Socket Class.
- Monitor for unexpected or out-of-specification CIP packets to CIP objects implemented in ControlLogix communications modules, including the Email Object and non-public vendor-specified objects.
- Monitor for unknown scanning on a network for Common Industrial Protocol (CIP)-enabled devices.
- Monitor for unscheduled firmware updates or logic downloads.
- Monitor for unexpected disabling of secure boot options.
- Monitor for arbitrary writes to communication module memory or firmware.
- Monitor for uncommon firmware file names.

Defenders should know what normal looks like for their ICS/OT environments, and regularly monitor for deviations in network activity with ICS/OT protocol aware technologies. Dragos customers receive the benefit of this intelligence and related controls as they are incorporated into the Dragos Platform (which was leveraged by OT Watch for threat hunting), into Neighborhood Keeper for community visibility, and provided as part of Professional Services engagements during related assessments.

Reference the five critical controls for OT cybersecurity identified by the SANS Institute for a framework for defending against adversary activity directed against ICS/OT environments.

Join Our Intel Briefing

Register now for a behind-the-scenes look at how we approach operationalizing threat intelligence using the recently disclosed Rockwell Automation ControlLogix firmware vulnerabilities.

Register Today

Ready to put your insights into action?

Take the next steps and contact our team today.

CONTACT US TODAY