APT Exploit Targeting Rockwell Automation Flaws Threatens Critical Infrastructure

By Eduard Kovacs ⋮⋮ 7/13/2023

An unnamed advanced persistent threat (APT) group has set its sights on two Rockwell Automation product vulnerabilities that they could use to cause disruption or destruction in critical infrastructure organizations.

According to its advisory (only accessible to registered users), Rockwell has worked with the US government to analyze what it describes as a new exploit capability leveraging vulnerabilities in ControlLogix EtherNet/IP communication modules.

Specifically, 1756 EN2 and 1756 EN3 products are impacted by CVE-2023-3595, a critical flaw that can allow an attacker to achieve remote code execution with persistence on the targeted system by using specially crafted Common Industrial Protocol (CIP) messages. A threat actor could exploit the vulnerability to modify, block or exfiltrate data passing through a device.

1756-EN4 products are impacted by CVE-2023-3596, a high-severity denial-of-service (DoS) bug that can be exploited using specially crafted CIP messages.

Rockwell Automation has released firmware patches for each impacted product and has shared potential indicators of compromise (IoCs), as well as detection rules.

“We are not aware of current exploitation leveraging this capability, and intended victimization remains unclear,” Rockwell said. “Previous threat actors cyberactivity involving industrial systems suggests a high likelihood that these capabilities were developed with an intent to target critical infrastructure and that victim scope could include international customers. Threat activity is subject to change and customers using affected products could face serious risk if exposed.”

The US Cybersecurity and Infrastructure Security Agency (CISA), which has helped Rockwell investigate the exploits, has also released an advisory to warn organizations about the vulnerabilities.

Industrial cybersecurity firm Dragos has also analyzed the vulnerabilities and the exploit, warning that it could — depending on the targeted ControlLogix device’s configuration — allow attackers to cause “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 said the exploit capability appears to be the work of an unnamed APT, but the company has found no evidence of exploitation in the wild to date, and it’s unclear what organizations or sectors may be targeted.

However, the company compared the type of access provided by CVE-2023-3595 to the zero-day flaw leveraged by a Russia-linked state-sponsored group in attacks involving the Trisis/Triton malware.

“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,” Dragos explained.

The company noted, “Knowing about an APT-owned vulnerability before exploitation is a rare opportunity for proactive defense for critical industrial sectors.”

News of the exploits emerged just weeks after it was reported that several US government departments had been investigating Rockwell’s operations at a facility in China, where employees might have access to information that could be used to compromise the systems of the company’s customers.

There has been some concern that employees could find vulnerabilities in Rockwell products and exploit them in zero-day attacks aimed at systems in the US.

Written By Eduard Kovacs

Eduard Kovacs (@EduardKovacs) is a managing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.