06 October 2023

MCB 01-23: Threats to OT and Shoreside Transportation Operations

REPORTED CYBER INCIDENT: ESTES EXPRESS LINES

Estes Express Lines is reporting an IT outage that appears to be the result of a cyber incident. Estes is a Less-than-Truckload (LTL) shipping company headquartered in Richmond, VA that specializes in regional, domestic, and international shipping. They are the fourth-largest LTL shipping company by sales in the U.S. and provide service to many entities within the MTS. ***Though Estes does not operate any Maritime Transportation Security Act regulated facilities, downstream effects potentially involve MTS partners.***

Incident Details

While the company has acknowledged a cyber incident, they have not released specific details about the incident or what has been compromised. They are asking customers to schedule pickups by contacting their account manager or completing a form on the company's website. Publicly available information regarding the incident is below:

- On 020CT23, Estes Express Lines released the following information via social media: "We are currently experiencing an outage in our core IT infrastructure, and it is impacting a number of our systems. We are working as fast as we can to resolve these issues and will keep you informed as to our progress. Please reach out to your account manager, preferably by text, with any questions or concerns, including pickups for today."
- On 030CT23, Estes Express Lines released the following statement via social media: "Yesterday we shared notice regarding an ongoing IT infrastructure outage and can confirm today that this outage appears to be the result of a cyberattack. We are unable to share specific details at this time, our terminals and drivers are effectively picking up and delivering freight while we work through this event."

Incident Summary

- Estes Express Lines is reporting an IT outage beginning on October 2nd, 2023, which appears to be the result of a cyber incident.
- The potential downstream effect of the Estes Express Lines cyber incident is not entirely known, but the company does provide shipping services to many Marine Transportation System (MTS) entities and could disrupt the movement of cargo.
- MTS stakeholders are advised to closely monitor official updates from Estes Express Lines.

If you have any questions, please visit our website at: https://www.uscg.mil/MaritimeCyber or reach out to MCRB at: maritimecyber@uscg.mil

VULNERABILITIES AFFECTING ROCKWELL AUTOMATION PRODUCTS

On July 12th, 2023, Rockwell published an alert presenting multiple vulnerabilities with potential implications to Liquefied Natural Gas (LNG) infrastructure and operations. Recent intelligence summaries from the Federal Energy Regulatory Commission detail developments in the cybersecurity landscape surrounding Rockwell Automation products, more specifically the **ControlLogix communication modules**. Organizations should consider the following key points:

- Common Vulnerabilities and Exposures: Two vulnerabilities, namely CVE-2023-3595 and CVE-2023-3596, have been identified with a Common Vulnerability Scoring System v3 score of 9.8, indicating their critical nature. These vulnerabilities are exploitable remotely with low attack complexity.
- Potential Impact: The exploitation of these vulnerabilities could result in denial or loss of control, denial or loss of view, theft of operational data, or manipulation of control, potentially leading to disruptive or destructive consequences in industrial processes.
- Affected Communications: These vulnerabilities affect ControlLogix Ethernet/IP (ENIP) communication modules present in various industrial sectors, including LNG. However, the specific targets remain unknown.

Best Practices

Since the July 12 alert, Rockwell Automation has released firmware updates to address these vulnerabilities. Additionally, CISA has published an ICS advisory recommending the following three actions:

- 1. Update Firmware.
- 2. Properly Segment Networks.
- 3. Implement Detection Signatures.

For more information, such as a full list of products affected and recommended detection rules, please see Rockwell Automation and CISA's Security Advisories.

SOURCES

"Rockwell Automation Select Communication Modules | CISA." 2023. Cybersecurity and Infrastructure Security Agency CISA. July 12, 2023. https://www.cisa.gov/news-events/ics-advisories/icsa-23-193-01.